Fraunhofer

FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE



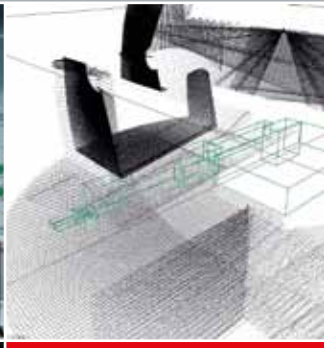







JAHRESBERICHT 2011







VORWORT

Sehr geehrte Leserinnen, sehr geehrte Leser,

wir freuen uns, für diesen Jahresbericht einen Moment innezuhalten und Höhepunkte des Jahres 2011 vorzustellen. In diesem Bericht finden Sie eine Auswahl von aktuellen Forschungsprojekten im Fraunhofer FKIE.

Das Institut mit seinem ausgeprägten Profil für Verteidigung und öffentliche Sicherheit hat sich im Jahr 2011 richtig in der Fraunhofer-Gesellschaft etabliert und fühlt sich zu Hause bei Europas führendem anwendungsorientiertem Forschungsdienstleister. Seit dem Jahr 2010, dem ersten Jahr als Fraunhofer-Institut, sind unsere Tätigkeitsfelder erheblich gewachsen. Wir konnten unsere Forschung für zivile Auftraggeber stark ausbauen und dem Bundesministerium der Verteidigung sowie dem nachgeordneten Bereich unverändert als unabhängiger und kompetenter Berater sowie Dienstleister zur Verfügung stehen. Unsere Erfahrung und Kompetenz in Sicherheitsfragen führte außerdem zu einem deutlichen Ausbau der Kooperation mit der Polizei des Bundes und der Länder. Die Technologien, die im FKIE entwickelt werden, helfen Bedrohungen für Menschen, Unternehmen, Gesellschaft und Staat abzuwenden.

Ein Beispiel ist Forschung im Bereich IT-Sicherheit – ein Kerngebiet des Instituts, das wir weiter ausbauen werden. An relevanten Themen, u.a. Botnetzen, wird abteilungsübergreifend geforscht; Kunden und Partner kommen aus der Privatwirtschaft sowie von Bund und Ländern, betreffen doch die Auswirkungen von Cyberangriffen gleichermaßen den zivilen wie den militärischen Sektor. So arbeiten das Bundesamt für Sicherheit in der Informationstechnik und das Fraunhofer FKIE im eng zusammen und haben die Kooperation im vergangenen Jahr noch intensiviert. Die gute Vernetzung mit Unternehmen spiegelt sich auf der anderen Seite wider in der kürzlich erfolgten Berufung von Herrn Thomas Tschersich, IT-Sicherheitschef der Deutschen Telekom, in unser Kuratorium.

Auch die traditionell schon gute Anbindung des Fraunhofer FKIE an die Universität Bonn und an die RWTH Aachen konnte noch weiter ausgebaut werden. Wir freuen uns, dass wir für die Abteilung Ergonomie und Mensch-Maschine-Systeme Herrn Prof. Dr.-Ing. Frank Flemisch als Abteilungsleiter gewinnen konnten. Prof. Flemisch ist neben seiner Funktion als Abteilungsleiter am FKIE als Professor für Systemergonomie am Institut für Arbeitswissenschaft (Leitung: Prof. Schlick) der RWTH Aachen tätig. Kurz vor Drucklegung des Jahresberichts erreichte die Institutsleitung zudem die erfreuliche Nachricht, dass Dr. Michael Meier den Ruf auf die gemeinsam mit dem FKIE eingerichtete Professur IT-Sicherheit am Institut für Informatik 4 (Leitung: Prof. Martini) der Universität Bonn angenommen hat. Herr Meier hatte diese Professur bereits seit April 2011 vertreten und wesentlich am Ausbau der Aktivitäten in den Bereichen Sicherheits-Monitoring sowie Bekämpfung von Schad-Software mitgewirkt.

Abschließend möchten wir den Mitarbeiterinnen und Mitarbeitern des Instituts unseren besonderen Dank aussprechen. Sie haben durch ihre vielfältigen Ideen und ihr vorbildliches Engagement ganz wesentlich zur qualitativen und quantitativen Entwicklung des Instituts im Berichtsjahr beigetragen. Nicht nur mit beeindruckenden wissenschaftlichen Beiträgen und der Entwicklung von wegweisenden Technologien, sondern auch mit ihrem hohen Einsatz bei der Bereitstellung der erforderlichen Infrastruktur in Verwaltung und Technik machen sie unsere Erfolge erst möglich.

Prof. Dr. Peter Martini
Institutsleiter

Prof. Dr. Christopher Schlick
Stellv. Institutsleiter

INHALTSVERZEICHNIS

INHALT

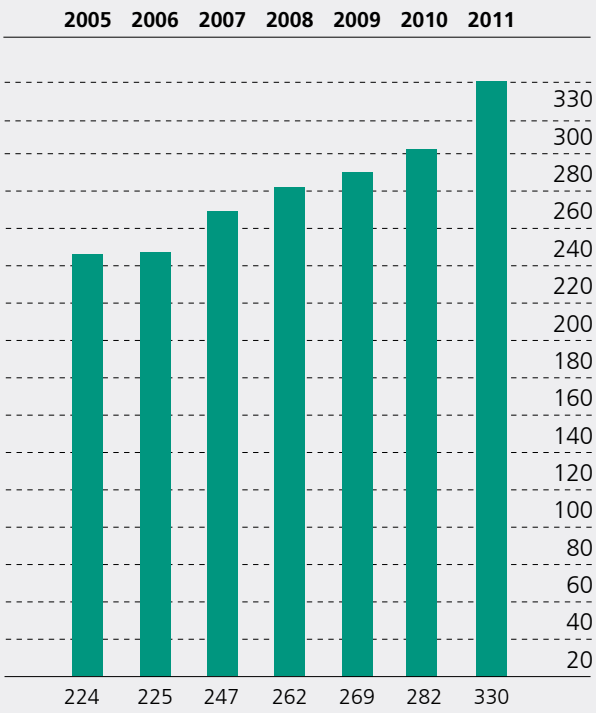
MIT HIGHTECH MENSCHEN IM EINSATZ UNTERSTÜTZEN

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE betreibt Forschung für Verteidigung, Sicherheit und Krisenreaktion. Stets geht es dabei um die Entwicklung und Verbesserung von Technologien zur Erkennung, Aufklärung und Abwehr von Gefahren – zu Boden, zu Wasser und in der Luft. So entstehen Konzepte und moderne Informations- und Kommunikationssysteme, die ein gemeinsames Ziel verfolgen: Menschen im Einsatz zu unterstützen.

Fraunhofer FKIE im Profil

Als Forschungsinstitut arbeitet das Fraunhofer FKIE für die Bundeswehr, zivile Sicherheitsbehörden und die Industrie. Sicherheitsrelevante Technologien und die Verbesserung der wehrtechnischen Systeme zur Vernetzten Operationsführung NetOpFü stehen im Mittelpunkt. Informationen gewinnen, übertragen, verarbeiten, darstellen und schützen – dies sind die Kernaufgaben des Fraunhofer FKIE. Der Erfüllung dieser Aufgaben dienen Führungsinformationssysteme, die ein exaktes Lagebild erstellen, indem sie die Verarbeitungskette vollständig abdecken. Wissensbasierte Assistenzsysteme, die komplexe Informationen und Kontextwissen verknüpfen und visualisieren, unterstützen Entscheidungen im militärischen Führungsprozess. Eigens entwickelte Schnittstellen sowie Verfahren der Augmented Reality fördern die schnelle und sichere Kommunikation zwischen Mensch und Technik.

Fraunhofer FKIE:
Entwicklung der Mitarbeiterzahlen 2005 – 2011



Die Spezialisierung auf die Entwicklung innovativer Technologien für wehrtechnische Systeme im Bereich Kommunikationsnetze, Informationsverarbeitung und Ergonomie kommt auch einer Vielzahl ziviler Anwendungen zugute. Die Nutzung von Synergieeffekten zwischen militärischer und ziviler Welt beschreibt den vom Fraunhofer FKIE gelebten »Bridging Technologies« Ansatz. Wichtigster Auftraggeber des Fraunhofer FKIE ist das Bundesministerium für Verteidigung, das auch für die Grundfinanzierung des Instituts sorgt. Das Fraunhofer FKIE kooperiert in einem ausgewählten Spektrum mit anderen Forschungseinrichtungen auf nationaler und internationaler Ebene. Das Institut ist eingebunden in die Forschungsorganisationen der NATO und der Europäischen Union. Darüber hinaus arbeitet das Fraunhofer FKIE mit zahlreichen Universitäten und industriellen Partnern zusammen. Am Fraunhofer FKIE arbeiten etwa 340 Mitarbeiterinnen und Mitarbeiter in Wachtberg und Bonn. Der Etat im Jahr 2011 betrug ungefähr 24 Mio €.

Die Marschrichtung lautet Anwendungsorientierung

Die Forschungsarbeit des Fraunhofer FKIE unterteilt sich in sechs hoch spezialisierte Abteilungen und Forschungsgruppen, wobei je nach Anforderung Projektteams interdisziplinär zusammengestellt werden. Allen gemein ist die hohe Anwendungs- und Kundenorientierung. Der Ankerpunkt jeder Projektidee bildet somit den Nutzen eines Systems im Einsatz. Die Forschungsergebnisse stützen sich auf selbst entwickelte Algorithmen und ausführliche Simulationsuntersuchungen, die Praxistauglichkeit wird an Demonstratoren erprobt und mit dem Auftraggeber eng abgestimmt. So entstehen in kürzester Zeit lauffähige Prototypen und nutzbringende Anwendungen.

ABTEILUNGEN UND FORSCHUNGSGRUPPEN

SENSORDATEN- UND INFORMATIONSFUSION / SDF

Kognitive Tools für intelligenten Überblick

Angesichts aktueller Sicherheitsanforderungen stößt der Mensch an die natürlichen Grenzen seines Wahrnehmungsspektrums und seiner Konzentrationsfähigkeit. Moderne, multisensorielle Aufklärungssysteme helfen, die Sensordaten und Informationen auszuwerten und zu handhabbarem »Wissen« zu verdichten. Hier spricht man von Datenfusion, die als ingenieurwissenschaftliche Disziplin das Ziel verfolgt, die menschliche Verknüpfungsleistung, etwa unterschiedlicher Sinneswahrnehmungen mit Erfahrungen oder Mitteilungen, zu verstehen, zu automatisieren und durch leistungsfähige Algorithmen zu steigern und neue Informationsquellen einzubeziehen.

KOMMUNIKATIONSSYSTEME / KOM

Unter allen Umständen zuverlässig kommunizieren

Ziel der Forschungsabteilung Kommunikationssysteme ist die Schaffung zuverlässiger und sicherer Verbindungen, denn in Krisen- und Bedrohungslagen ist der reibungslose Informationsaustausch zwischen den Einsatzkräften entscheidend. Um selbst unter widrigen Kommunikationsbedingungen eine robuste Informationsübertragung sicherzustellen, bedarf es eines ganzheitlichen Forschungsansatzes: Dieser reicht von den elementaren physikalischen Eigenschaften der Funkwellenausbreitung über Modulations- und Multiplexverfahren bis hin zu höheren Protokollschichten und Netzmanagement.

INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME / ITF

Damit alle Einsatzkräfte im Bilde sind

Einen Forschungsschwerpunkt bilden seit Jahren Verfahren und Technologien zur Erzeugung eines einheitlichen und aktuellen Lagebildes. Dies dient für alle beteiligten Einsatzkräfte als Grundlage für die Beurteilung einer Situation und ermöglicht adäquate Handlungsentscheidungen. Die Anforderungen an solche Systeme sind hoch, müssen sie doch über Sprach- und Systemgrenzen hinaus funktionieren und den situationsangepassten Informationsaustausch mit dynamisch wechselnden Partnern ad hoc unterstützen. Die dazu gehörenden Führungsinformations- und Assistenzsysteme werden mit Blick auf diese Anforderungen entwickelt und in Feldversuchen geprüft. Auch im zivilen Umfeld, etwa nach Naturkatastrophen, können sie Krisenreaktionskräfte bei der Planung und Durchführung ihrer Einsätze unterstützen.

ERGONOMIE UND MENSCH-MASCHINE-SYSTEME / EMS

Mensch und Technik systemisch integrieren

In Gefahren- und Stresssituationen steigt der Anspruch an hochkomplexe Technologien vor allem im Hinblick auf ihre einfache und intuitive Bedienbarkeit - vor Ort und mobil. Der Forschungsbereich

Ergonomie und Mensch-Maschine-Systemtechnik hat sich darauf spezialisiert, komplexe Lagebilder und Führungsprozesse für den Menschen möglichst eindeutig und transparent darzustellen. Für den mobilen Einsatz erweitert sich die Forschung um virtuelle Simulation oder Augmented Reality, also der technologischen Anreicherung der Realität um Zusatzinformationen. Ein besonderer Fokus liegt auf innovativen Verfahren zur Informationsübermittlung bei der Telearbeit und -kooperation. Die Betrachtung von Mensch und Technik als Einheit und die Zusammenführung in einem flexiblen Mensch-Maschine-System gewährleistet die effektive Interaktion der Akteure.

UNBEMANNTE SYSTEME / US

Funktionieren, wo es für Menschen zu gefährlich ist

Dort, wo es für Menschen eine zu große Gefahr bedeuten würde, selbst tätig zu werden, unterstützen mobile Roboter etwa beim Aufspüren giftiger Substanzen in Industrieanlagen oder beim Aufbau eines Kommunikationsnetzes in einem Krisengebiet. Die Forschungsgruppe Unbemannte Systeme schafft dafür die technischen Grundlagen und sichert zudem die einfachere und intuitivere Handhabung komplexer Mehrrobotersysteme.

Mit Assistenzfunktionen sowie Koordinationsverfahren geht das Fraunhofer FKIE das Thema auf zwei Ebenen an. Hier entstehen Algorithmen, die Sensordaten verarbeiten, Vorgänge automatisieren und Handlungsvorschläge generieren, so dass die Operateure Entlastung erfahren und sowohl die Grundlage als auch die Freiräume für essenzielle Entscheidungen gewinnen.

CYBER DEFENSE / CD

Virtuelle Sicherheit mit handfestem Nutzen

Die digitale Vernetzung birgt viele Risiken. Dazu zählen auch Angriffe im virtuellen Raum. Die dagegen notwendigen Verteidigungsstrategien entwickelt die Forschungsgruppe Cyber Defense. Hier werden die Vertrauenswürdigkeit von Computersystemen und -netzen beurteilt, Gefährdungspotenziale abgeschätzt, Ursachen für Cyber- Angriffe analysiert und entsprechende leistungsfähige Warn- und Schutzmechanismen entwickelt.

Das oberste Ziel lautet: Entscheidungsträgern in allen Bereichen netzbasierter Aufklärung und Operationsführung konkrete Unterstützung in Sachen IT-Sicherheit zu bieten: Etwas, das auch Wirtschaftsunternehmen immer häufiger nachfragen.

Das Portfolio von Cyber Defense bietet einerseits technische Lösungen und Studien, inklusive Anforderungsanalysen, Machbarkeitsstudien und anwendungsorientierte Demonstratoren. Andererseits profitieren die Auftraggeber von Dienstleistungen, in Form von Schulungen oder unabhängigen wissenschaftlich- technischen Projektbegleitungen, Gutachten und Untersuchungen.

ANSPRECHPARTNER IM FRAUNHOFER FKIE

Institutsleiter
Prof. Dr. Peter Martini
Telefon 0228 9435-287
peter.martini@fkie.fraunhofer.de

Sensordaten- und Informationsfusion

Abteilungsleiter
Priv.-Doz. Dr. Wolfgang Koch
Telefon 0228 9435-373
wolfgang.koch@fkie.fraunhofer.de

- Ortung und Navigation
- Weiträumige Überwachung
- Bedrohungserkennung

Kommunikationssysteme

Abteilungsleiter
Dr. Markus Antweiler
Telefon 0228 9435-811
markus.antweiler@fkie.fraunhofer.de

- Aufklärung und Störung
- Software Defined Radio
- Robuste heterogene Netze

Forschungsgruppenleiter
Dr. Jens Tölle
Telefon 0228 9435-513
jens.toelle@fkie.fraunhofer.de

Cyber Defense

Stellv. Institutsleiter
Prof. Dr. Christopher Schlick
Telefon 0228 9435-287
christopher.schlick@fkie.fraunhofer.de

Informationstechnik für Führungssysteme

Abteilungsleiter
Dr. Michael Wunder
Telefon 0228 9435-511
michael.wunder@fkie.fraunhofer.de

Verteilte Führungsinformationssysteme

Wissensmanagement und Assistenzsysteme

Wissensbasierte Informationsanalyse

Ergonomie und Mensch-Maschine-Systeme

Abteilungsleiter
Prof. Dr. Frank Flemisch
Telefon 0228 9435-573
frank.flemisch@fkie.fraunhofer.de

Systemtechnik

Human Factors

Unbemannte Systeme

Forschungsgruppenleiter
Dr. Dirk Schulz
Telefon 0228 9435-483
dirk.schulz@fkie.fraunhofer.de

Windparks in der Ostsee: Ortsfeste »Bewegtziele« wie Windräder erscheinen auf dem Radar als Geisterziele.

Rechts: Visualisierungssoftware Geo4T von Schönhofer Sales & Engineering GmbH.

RADAR OHNE RADAR

Das Fraunhofer FKIE hat Verfahren zur Ortung von Schiffen und Flugzeugen entwickelt, die ohne Radar auskommen. Sie funktionieren mit Signalen, die es quasi als Abfallprodukt kostenlos gibt.

Radaranlagen haben keinen guten Ruf in der Bevölkerung. Die Furcht vor der vermeintlich gesundheitsschädlichen Strahlung hat dazu geführt, dass Radareinrichtungen, die Flugzeuge oder Schiffe orten sollen, heute kaum noch genehmigungsfähig sind. Auch aus Sicht militärischer Nutzer hat Radar einen großen Nachteil: Weil es Signale aussendet, ist es selbst leicht zu orten und im Verteidigungsfall erstes Ziel des Gegners.

Eine Alternative ist das passive Radar: Es nutzt vorhandene Funksignale zu Ortung. Ein zusätzlicher Sender ist überflüssig, deshalb bedarf es auch keiner langwierigen Genehmigungen und es gibt keine Einwände aus der Bevölkerung. Nachteil: Die Signale sind für ganz andere Zwecke gedacht – etwa für die Sprachkommunikation – und damit eigentlich ungeeignet für die Lokalisierung von Objekten. In den letzten Jahren gab es jedoch deutliche technische Fortschritte. Neben einigen Unternehmen und Forschungsinstituten, die an dem Thema arbeiten, ist es vor allem die Abteilung Sensordaten- und Informationsfusion des Fraunhofer FKIE, die das Thema derzeit wissenschaftlich vorantreibt. Das Institut verfolgt dabei zwei Ansätze: die Ortung mit Echos von GSM-Mobilfunksignalen beziehungsweise mit Messungen von bekannten Signalen, die von den Objekten selbst ausgesandt werden.

Ortung mit Mobilfunksignalen

Die Fledermaus macht es vor: Die Flugsäuger senden hochfrequente akustische Signale aus und orientieren sich am Echo, das von Bäumen oder Beute zurückgeworfen wird. Nach dem gleichen Prinzip – nur mit elektromagnetischen Impulsen – funktioniert das Radar. Doch Radarsignale sind heute nicht mehr die einzige Option, um Echos zu erzeugen. Der Äther ist voll mit elektromagnetischen Signalen, von langwelligen Rundfunksignalen bis zu Mikrowellen. Im Prinzip könnte man sich aus diesem Spektrum bestimmte Signale aussuchen und diese zur Echoortung zweckentfremden.

Genau diese Idee verfolgt Ulrich Nickel aus der Abteilung Sensordaten- und Informationsfusion des Fraunhofer FKIE. Ganz neu ist das Konzept nicht, es wurde bereits mit Radio- und Fernsehsendern versucht. Doch die gibt es nicht überall – im Gegensatz zu den GSM-Mobilfunkbasisstationen. Heute gibt es in fast jeder Gegend Europas ein dichtes Netz solcher Mobilfunksender, deren Position metergenau bekannt ist. Sie könnten gut geeignet sein, um das Fledermausprinzip auch zur Positionsbestimmung von Schiffen oder Flugzeugen zu verwenden. Einziger Unterschied: Die Fledermaus (der Mobilfunksender) wird festgehalten, der Baum (das Schiff) bewegt sich. Die Mobilfunksignale sind gesundheitlich unbedenklich und obendrein sind sie kostenlos.

Tatort Ostsee

Dass das PCL-Prinzip (Passive Coherent Location) tatsächlich funktioniert, hat Nickel und seine Gruppe 2011 an der Ostseeküste vor der Insel Fehmarn getestet. Damit wurde dieses Konzept zum ersten Mal in einem vollständigen PCL-System erfolgreich umgesetzt. Die Ostsee war deshalb erste Wahl, weil es dort keine lückenlose Überwachung der Schiffe gibt. Zwar übermitteln die Schiffe ihre Position mit dem AIS-Signal (Automatisches Identifikationssystem), doch das ist unzuverlässig. Wer etwas zu verbergen hat, kann eine Software kaufen, die die Positionsangaben verfälscht. So können etwa Tanker Öl ablassen und dabei eine ganz andere Position vortäuschen. Das macht es den Behörden fast unmöglich, die wahren Täter zur Rechenschaft zu ziehen. Der Ortung mit Mobilfunksignalen können sie dagegen nicht entgehen. Die Signale sind immer da und ihre Reflektion an einem Schiffsrumpf lässt sich nicht unterdrücken.

Die festen Basisstationen sind als Sender ideal, weil ihre Position exakt bekannt ist. Im Prinzip wäre es aber auch möglich, mobile

Basisstationen zu nutzen, etwa in abgelegenen Regionen, wo es keine festen Stationen gibt, wo aber schnell eine Ortung aufgebaut werden muss. Auch der Empfänger, der in Nickels Experiment fest installiert war, ist im Prinzip mobil. Nur wenige Minuten dauert es, bis Sender oder Empfänger aufgebaut und ihre Position mittels GPS bestimmt sind.

Die Ortung der Ziele lässt sich verbessern, wenn mehrere Basisstationen benutzt werden, die möglichst gut um das zu beobachtende Gebiet verteilt sind. Bei der Auswahl der Stationen und der Position des Empfängers ist zu bedenken, dass der Empfänger für Echos blind ist, die vom Schiff in Richtung des Senders zurückgeworfen werden. Durch gleichzeitige Benutzung anderer Sender lässt sich dies aber leicht beheben. Insgesamt nutzte das FKIE-Team sieben GSM-Basisstationen an der Küste. Der Empfänger wurde in einem Bundeswehrstandort in Staberhuk errichtet, von wo aus der Schiffsverkehr in der Lübecker Bucht und im Fehmarn Belt überwacht werden konnte.

Als Empfänger diente im Test ein Experimentalsystem mit 16 Signalkanälen, das selbst schwache Signale empfängt. Weil die Aufzeichnungsdauer auf 13 Sekunden begrenzt und damit viel zu kurz ist, hat das Fraunhofer FKIE mit der Firma Schönhofer in Siegburg einen neuen Empfänger namens ECHSE-2 mit ebenfalls 16 Kanälen entwickelt. Die Daten werden auf einer Festplatte abgelegt, so sind Aufzeichnungen von mehreren Stunden möglich. Die Geschwindigkeit der Schiffe wird über das Doppler-Prinzip bestimmt: Bewegt sich ein Objekt, wird die Frequenz des zurückgeworfenen elektromagnetischen Signals höher oder niedriger – wie der Schall bei einem Polizeiauto mit Martinshorn, das an einem vorbeifährt.

Auf 200 Meter genau

Wie genau ist das passive Mobilfunk-Radar? Vergleiche mit den AIS-Signalen der Schiffe in der Lübecker Bucht zeigen, dass sich die Ortungsgenauigkeit nach einigen Minuten auf etwa 200 Meter einpendelt. Das System braucht eine gewisse Anlaufphase, weil die Software erst anhand von Bewegungsmustern erkennen kann, ob ein Echosignal von einem Schiff kommt oder ob es ein Geistersignal von einem festen Objekt ist, etwa von einem Windrad. Windrotoren bewegen sich ebenfalls und stören die Erfassung. Die Bewegungsmodelle in der Software sind aber so ausgereift, dass sie diese unerwünschten Echos ausschließen.

Eine knifflige Aufgabe, die das Programm mittlerweile gut meistert, ist die Trennung mehrerer Schiffe, deren Routen sich kreuzen. Andere Programme verwechseln leicht die Objekte. Auf dem Bildschirm sieht es dann so aus, als würden die Schiffsrouten abknicken. Das Bewegungsmodell, das am Fraunhofer FKIE entwickelt wurde, verhindert solche Fehlinterpretationen. Kreuzen sich zwei Schiffe, verschmelzen ihre Piktogramme in der Karte zu einem Symbol, um sich kurze Zeit später wieder zu trennen. Das mathematische Modell weist dann jede Spur wieder dem richtigen Schiff zu.

Ortung von Transpondersignalen

Die einfachste Möglichkeit, ein Flugzeug zu orten, ist ADS-B (Automatic Dependent Surveillance Broadcast). Moderne Verkehrsflugzeuge haben einen Sender eingebaut, der laufend Position und Flughöhe aussendet und so eine ständige Ortung ermöglicht. Das System findet immer mehr Verbreitung und soll die herkömmliche Radarortung ergänzen. Die ist auch im dichten europäischen Luftverkehr lückenhaft. Während die Radarortung an Flughäfen sehr präzise ist, gibt es weiter davon entfernt weiße Flecken. ADS-B ist also für die Flugsicherung eine wichtige Informationsquelle – die allerdings nicht hundertprozentig vertrauenswürdig ist. Der Sender kann von Luftpiraten gestört oder ganz abgeschaltet werden.

Zur Positionsbestimmung nutzt das ADS-B zudem die Signale der GPS-Satellitennavigation. Doch GPS ist nach wie vor ein militärisches System in Händen der USA, die dieses im Fall von militärischen Konflikten jederzeit abschalten kann. Auch ist bekannt, dass sich das GPS-Signal gezielt manipulieren lässt.

Dem Inhalt der ADS-B-Signale kann man also nicht unbedingt vertrauen. Umso vertrauenswürdiger ist das Signal selbst. Egal welche Information sie übermitteln, die Signale haben immer eine festgelegte zeitliche Struktur, die man nicht fälschen kann. Kennt man die Laufzeit des Signals vom Flugzeug zur Antenne, kann man daraus auf die Entfernung schließen. Fängt man dasselbe Signal mit mindestens vier Empfängern an unterschiedlichen Positionen auf, lässt sich mittels einfacher Geometrie ein eindeutiger Schnittpunkt errechnen: die Position des Flugzeugs. Experten nennen solche Verfahren Laufzeit- beziehungsweise Laufzeitdifferenzverfahren. Bei diesen TOA- bzw. TDOA-Methoden, wobei die Kürzel für »Time of Arrival« beziehungsweise »Time-Difference of Arrival« (Differenz der Ankunftszeit) stehen, wird aus der Ankunftszeit oder der Differenz der Ankunftszeit des Signals auf die Position des Senders geschlossen. Gesucht wird also nach den Zeitunterschieden, mit denen die Signale bei den unterschiedlichen Empfängern eintreffen. Im Grunde funktionieren diese Methoden wie ein umgekehrtes GPS. Während bei der Satellitennavigation die Position der Sender in den Satelliten bekannt ist und die Position des Empfängers – etwa des Navigationssystems im Auto – gesucht wird, ist bei der TOA/TDOA-Ortung die Position der vier (oder mehr) Empfänger bekannt und die Position des Senders wird gesucht. Geometrisch ist das Prinzip aber vergleichbar.

Riesiges Testfeld

Für einen Feldtest des Fraunhofer FKIE hat das Team von Klaus Wild vier Sensoren mit Abständen zwischen 8 und 13 Kilometern in der Nähe des Instituts in Wachtberg aufgebaut. Ziel war es, in einem Areal von 100 mal 100 Kilometern ADS-B Signale von Flugzeugen zu empfangen und mit den entwickelten Verfahren die Position des entsprechenden Flugzeugs zu bestimmen. Die Genauigkeit der Ortung liegt bei circa einem Kilometer – als

UMWELTSÜNDERN AUF DER SPUR

Dr. Ulrich Nickel ist Leiter des Projekts »Passive Lokalisierung mit GSM-Beleuchtern«. Von ihm stammt die Idee, Schiffe mit Echos von Mobilfunksignalen zu orten.

Wie kamen Sie auf die Idee der passiven Ortung mit Mobilfunksignalen?
Die Idee entstand vor etwa drei Jahren hier am Fraunhofer FKIE. Nach unserem Wissen sind wir die einzigen weltweit, die eine solches komplettes System in Betrieb haben.

Sie haben das Konzept vor Fehmarn getestet. Warum gerade dort?
Bundeswehr und Bundespolizei wünschen sich eine ergänzende Überwachungsensorik für den Küstenbereich. Insbesondere das zivile Systemen AIS ist leicht zu stören. Auch auf anderen Gewässern herrscht Bedarf danach, etwa im Mittelmeer, wo man zum Beispiel Umweltverschmutzer überführen möchte, die Öl ablassen und dabei eine falsche Position angeben.

Was sind Ihre nächsten Pläne?
Wir wollen 2012 noch Messungen am Bodensee machen und unser System mit anderen vergleichen. Unser Nachbarinstitut, das Fraunhofer FHR, verfolgt eine ähnliche Idee, allerdings mit Signalen des digitalen terrestrischen Rundfunks und Fernsehens. Und das EADS-Tochterunternehmen Cassidian hat ein ebensolches System und eines auf Basis von UKW-Radio. Beide nutzen unsere Software zur Datenfusion. Wir wollen herausfinden, wie sich die Systeme in verschiedenen Situationen bewähren und welchen Gewinn man durch Kombination mehrerer Verfahren erzielen kann.

Arbeiten Sie auch an einem kommerziellen Ableger?
Wir haben beim Bundesministerium für Bildung und Forschung im Verbund mit Cassidian und Fraunhofer FHR ein Projekt beantragt, um ein Backup-Ortungssystem für den Luftverkehr zu entwickeln. Es wäre ideal als bodennahes Radar und könnte das Primärradar ergänzen, das nur den oberen Luftraum erfasst.

Referenz dienten die Positionsdaten des ADS-B. Fügt man zu dem Sensornetz weitere Sensoren hinzu, lässt sich sowohl die Abdeckung als auch die Genauigkeit verbessern.

Die besondere Leistung des FKIE-Teams ist die Idee, die Signalstruktur zu nutzen, um an jedem Sensorknoten eine Ankunftszeitmarke zu bestimmen. Dieses Verfahren ermöglicht es, die Kommunikationsanforderungen im Sensornetz erheblich zu reduzieren. Jeder Sensor verarbeitet die empfangenen Nachrichten direkt vor Ort und überträgt anschließend nur noch die dekodierte Nachricht sowie eine entsprechende hochgenaue Empfangszeitmarke an eine Leitstelle. Die dekodierten Nachrichten und die zugehörigen Zeitmarken sind nur wenige Byte lang und lassen sich selbst bei regem Flugverkehr über Mobilfunk an eine Leitstelle senden.

Luftraumüberwachung für die Dritte Welt

In Europa ist das Fraunhofer FKIE eine von wenigen Forschungseinrichtungen, die sich derzeit mit einer Kombination von TOA/TDOA-Ortung befasst, welche die Signalstruktur von ADS-B Transpondernachrichten nutzt. Der Charme der FKIE-Lösung ist ihre Einfachheit. Zum Empfang genügen ein Sensor mit Antenne und ein Laptop mit UMTS-Stick. Selbst wenn man mit dem System ganz Deutschland abdecken wollte, wären die Kosten gering. Interessant ist das System nicht nur für die Überwachung des deutschen Luftraums, auch andere Länder oder Kontinente würden profitieren. So gibt es in weiten Teilen Afrikas überhaupt keine Überwachung des Luftraums. GSM-Mobilfunknetze gibt es dagegen mittlerweile selbst in abgelegenen Gegenden der Erde, so dass der Datenaustausch gesichert wäre.

In dem Projekt kooperiert das Fraunhofer FKIE mit einem Industriepartner. Die Kooperation soll den Ideenaustausch fördern und wenn möglich zu einem Produkt führen. Das hätte Potenzial auch in anderen Branchen. So ist das TOA/TDOA-Prinzip auch für die Ortung in Gebäuden geeignet, etwa von Containern oder Paketen, die mit entsprechenden Sendern ausgestattet sind. Auf hoher See könnte es die Positionsbestimmung von Schiffen anhand der AIS-Signale überprüfen – und wäre damit eine Ergänzung zur Ortung mit GSM-Signalen, die Klaus Wilds Abteilungskollege Ulrich Nickel untersucht.

Einsatzszenario für die FKIE-TDOA-Sensoren.

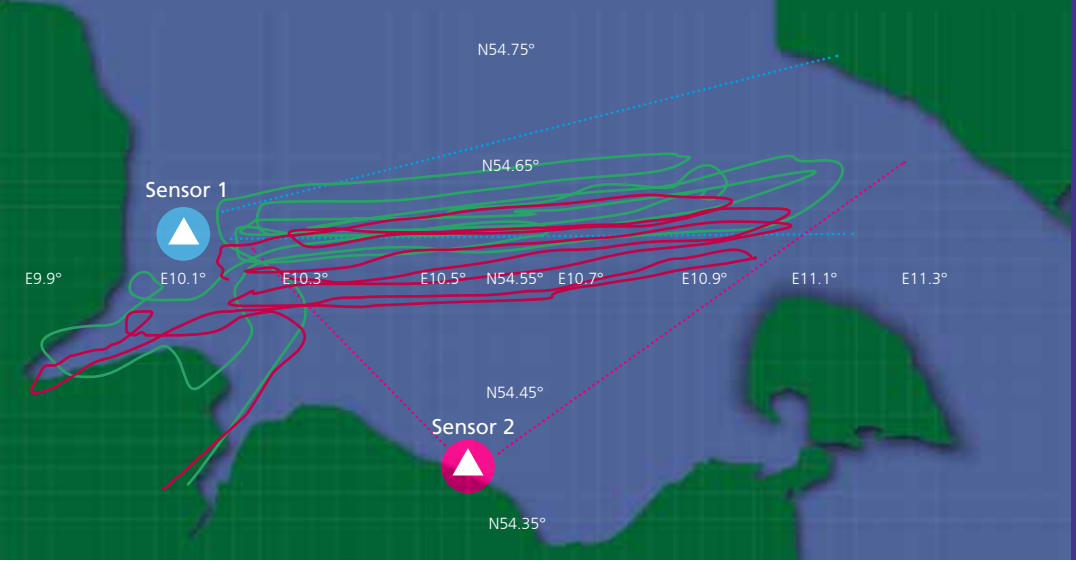
MIT DEM ZWEITEN SIEHT MAN BESSER

Bedrohungen von Schiffen schneller erkennen – die Fusion der Daten mehrerer Sensoren macht's möglich.

Was gibt eins plus eins? Mathematisch ist der Fall klar: zwei. Bei Einsätzen der Marine ist das leider nicht so klar. Wenn zwei Schiffe ein möglicherweise feindliches Objekt – zum Beispiel eine Rakete – verfolgen, verlässt sich jedes nur auf seine eigenen Sensordaten, wenn es Maßnahmen zum Selbstschutz ergreift. Wenn das Objekt auf das eigene Schiff zurast, ist das brandgefährlich. Denn frontal lassen sich Position und Geschwindigkeit der Rakete mittels Radar nur schwer bestimmen. Ein Wechsel der Perspektive würde helfen: Von der Seite beobachtet, ließen sich Geschwindigkeit und Ort des Flugobjekts viel leichter identifizieren. Doch das geschieht nicht, weil jedes Schiff autark ist und für seine Verteidigung in erster Linie seine eigenen Sensordaten nutzt. Eins plus eins macht in diesem Fall leider nur eins.

Vier Nationen haben sich in MPEC (Multiplatform Engagement Capability) zusammengeschlossen, um dieses Manko zu beheben. Ziel des Projekts ist es, Sensordaten aus den Schiffen eines Verbands so zu kombinieren, dass plattformübergreifende Lagebilder entstehen. Das Prinzip: Alle Schiffe geben ihre Daten an die Nachbarschiffe weiter und können daraus ein Lagebild berechnen, das dank der fusionierten Daten erheblich detailreicher ist. Wo befindet sich mein Schiff, wo sind

Fregatte 124 (Sachsen-Klasse) beim Abschuss einer Boden-Luft-Rakete.



Aufgezeichnete Flugdaten der deutschen Seeübung.

die Schiffe meines Verbands, wo steht der Gegner? Solche Informationen und die daraus resultierenden Bedrohungen sollen sich aus dem Lagebild erschließen lassen und zwar präziser und schneller als bisher. Für Deutschland ist das Fraunhofer FKIE im Auftrag des Bundesamts für Wehrtechnik und Beschaffung mit von der Partie.

Schielende Sensoren

Die Fusion der Daten ist indes einfacher gesagt als getan. Schon die Kommunikation der Schiffe untereinander bereitet Probleme. Ist die Bandbreite zu gering, fehlen Datenpakete oder sie kommen leicht verzögert oder in der falschen Reihenfolge an. Zudem ist auf die Messungen nicht immer Verlass, die Navigationsdaten können ungenau sein oder die Sensoren zweier Schiffe »schielen« und liefern zwei Spuren, obwohl es sich nur um ein Objekt handelt. Ist eine Rakete im Anflug, können solche Fehler verheerend sein.

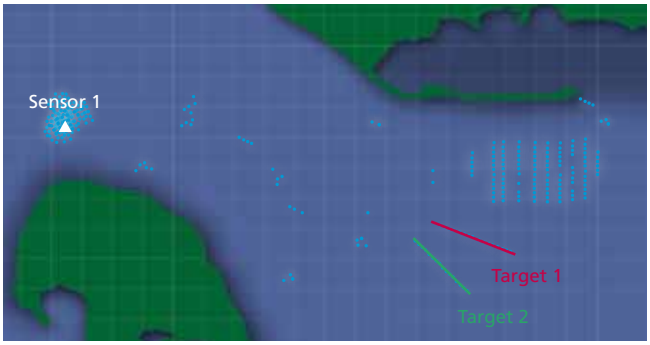
Das Team um Dr. Martin Ulmke, MPEC-Projektleiter am Fraunhofer FKIE, löst diese Schwierigkeiten mit mathematischer Raffinesse. Ein Schätzverfahren errechnet auf Basis von Wahrscheinlichkeitsdichten die Position eines Objekts und verfolgt es mit einem Bewegungsmodell. Das stellt sicher, dass das Objekt nicht vom Lagebild verschwindet, selbst wenn einmal kurzzeitig Daten fehlen. Auch wenn sich zwei Flugobjekte kreuzen, sorgt das Bewegungsmodell dafür, dass die Spuren konsistent bleiben und nicht etwa unsinnig abknicken.

Wie gut das funktioniert, hat Ulmkes Team anhand von realen Daten untersucht, die 2009 bei einer Seeübung in der Ostsee aufgezeichnet wurden. Die Übung wurde eigens für diesen Zweck ausgeführt und zwar so, dass die Daten möglichst knifflig zu fusionieren waren. Zwei Flugzeuge flogen komplizierte Manöver über dem Übungsort, darunter Parallelflüge und Kreuzungen. Verfolgt wurden die Flüge von zwei Radaranlagen der EADS-Tochter Cassidian – eine auf einem Schiff, eine zweite an Land. Ein Mitarbeiter des Fraunhofer FKIE befand sich an Bord des Schiffes und zeichnete die Daten auf.

See-Störungen unterdrückt

Die Ergebnisse sind vielversprechend: Die Kontinuität in der Spurverfolgung ist schon gut, auch das Unterdrücken von Störungen in den reflektierten Radarsignalen durch den Einfluss der Wasseroberfläche hat der Algorithmus gut im Griff. Mit mehr Sensordaten aus weiteren Radaranlagen oder anderen Sensoren ließe sich die Verfolgung der Flugrouten der Testflugzeuge aber noch steigern. Bevor MPEC 2012 endet, soll es im Lauf des Jahres noch einmal eine Seeübung in Frankreich geben, wo der verbesserte Algorithmus getestet wird. »Bis dahin wollen wir deutlich besser sein als die original Sensordaten«, verspricht Martin Ulmke.

Darüber hinaus möchte das Team gemeinsam mit der FKIE-Abteilung Kommunikationssysteme eine Simulation erstellen, mit der man den Datenaustausch zwischen den Schiffen realistisch durchspielen kann – mit allen Tücken wie begrenzter Bandbreite und langer Latenzzeit. Umgekehrt soll die Simulation Hinweise geben, wie die Kommunikationskanäle verbessert werden müssten, um eine verlässliche Datenfusion zu ermöglichen.



Aufgezeichnete Radardaten der deutschen Seeübung, aus denen Zielspuren zu extrahieren sind.

SIGNALE VON DER WEIDE

Das Fraunhofer FKIE untersucht, ob Windräder die Funkaufklärung stören. Die Gefahr besteht, doch häufig haben Störungen andere Ursachen.

Windräder verschandeln die Landschaft – diese Klagen hört man immer wieder von Bürgern, die in der Nähe von Windkraftanlagen wohnen. Ein weiterer, nicht so bekannter Einwand kommt von Sicherheitsdiensten. Sie befürchten, dass die Windräder hochfrequente Funksignale stören könnten. Die Störsignale würden den Empfang und dadurch die Aufklärung von Funkverkehr erschweren. Konkrete Klagen gab es über Kurzwellen-Empfangs- und Peileinrichtung. In den letzten Jahren sind die Störsignale merklich angestiegen. Bisher gab es aber keine verlässlichen Untersuchungen, ob die Störungen tatsächlich von den Windrädern kommen, oder ob es andere Ursachen gibt.

Messung der Abstrahlung von Windkraftanlagen im Kurzwellenbereich mit einer Rahmenantenne.

Um der Sache auf den Grund zu gehen, ist Stefan Hawlitschka von der Abteilung Kommunikationssysteme des Fraunhofer FKIE nach Euskirchen gefahren. Dort steht in der Nähe einer Einrichtung der Bundespolizei ein Windpark mit zehn Windturbinen des Typs Enercon E-53, wie man ihn so ähnlich häufig in Deutschland findet. Im Kofferraum hatte Hawlitschka eine Rahmenantenne und einen Spektrumanalysator von Rhode & Schwarz.

Störquelle Frequenzumrichter

Die schlechte Nachricht vorweg: Die Windkraftanlagen senden tatsächlich Störsignale aus. Quelle sind die Frequenzumrichter, die dafür sorgen, dass die Wechselspannung des Generators in der Gondel stabil an die Frequenz und die Spannung des Wechselspannungsnetzes angepasst wird. Die elektronischen Schaltungen erzeugen Rechtecksignale mit einer Anstiegszeit von einigen hundert Nanosekunden. Das hat eine Abstrahlung von Frequenzen zur Folge, die bis in das Frequenzspektrum von einigen Megahertz reichen. Mit seinem empfindlichen Messgerät konnte Hawlitschka in der Nähe des Turms sogar die Modulation der Signale hören, die durch das Vorbeistreichen der Rotorblätter am Turm erzeugt wird.

Weil die Schaltungen im unteren Teil des Turms untergebracht und gut abgeschirmt sind, dringt das Störsignal dennoch nur recht schwach nach außen. Die gute Nachricht lautet deshalb: Wenn die Windanlagen weit genug von Empfangsantennen entfernt errichtet werden, geht ihr Signal im Hintergrundrauschen unter. Ab einer Entfernung von 1,5 Kilometern konnte Hawlitschka die Störungen nicht mehr nachweisen.

Daraus folgt zweierlei: Weil mit einem weiteren massiven Ausbau der Windenergie zu rechnen ist, wäre es sinnvoll, Schutzzonen zu definieren. Sie könnten verhindern, dass die Windparks zu nahe an militärische oder zivile Empfangseinrichtungen heranrücken. Um diese Schutzzonen genauer zu definieren, bedarf es weiterer systematischer Messungen an anderen Windkraftanlagen in verschiedenen topographischen Gegenden und mit anderen Messvarianten. Unabhängig davon empfiehlt Stefan Hawlitschka den Herstellern von Windkraftanlagen zusätzliche Anstrengungen zur Abschirmung der Frequenzumrichter.

Schutzzonen nötig

Windkraftanlagen sind aber nur die Spitze des Eisbergs. Frequenzumrichter arbeiten überall, wo Strom aus erneuerbaren Energien erzeugt wird, etwa in Photovoltaik- oder Biogasanlagen. Auch dort hat Hawlitschka gemessen, allerdings weit geringere Störpegel gefunden. Dennoch müssen die Betreiber von Antennen zur Funkaufklärung mit einem auch in Zukunft wachsenden Störpegel rechnen. Autos, Küchengeräte, Schweißgeräte oder Industriemaschinen – sie alle senden Störsignale aus. Insbesondere die zunehmende Computervernetzung und der digitale Datenverkehr haben zu einer deutlichen Zunahme des Störpegels geführt. Planer sollten deshalb bei neuen Wohngebieten, Industrieanlagen oder Straßen Rücksicht auf die Bedürfnisse der Antennenbetreiber nehmen und Schutzzonen einhalten. Wegen des dichten Gedränges der Funkfrequenzen kommt es immer wieder zu Konflikten. Stefan Hawlitschka, der für das Fraunhofer FKIE in zwei Arbeitsgruppen der Bundesnetzagentur zu solchen Themen sitzt, kennt zum Beispiel den Fall, bei dem die deutsche Flugsicherung ihren Sprechfunk nicht mehr benutzen konnte, weil die Abstrahlung des TV-Kabels zu sehr störte.

Übrigens: Die untersuchten Störungen wurden nicht von Windkraftanlagen verursacht. Das Rätsel hatte eine überraschend einfache Lösung: Die Störungen stammen von elektrischen Weidezäunen, die mit kurzen Stromimpulsen die Tiere daran hindern, die Absperrung zu überwinden. Die Impulse entstehen in einer Funkenstrecke, die starke hochfrequente Störsignale abstrahlt. Das Problem ist seit längerem bekannt und eigentlich schien es gelöst, weil solche Anlagen innerhalb eines Schutzbereichs um die Empfangsanlage herum verboten sind. Neue Weidezäune arbeiten nach einem anderen Prinzip und senden keine Störungen aus. Doch offensichtlich nutzen viele Landwirte ihre alten Elektrozäune weiter, um sich die Anschaffung neuer Zäune zu sparen.

BEREIT FÜR ALLE VERBINDUNGEN

Das Fraunhofer FKIE berät die Bundeswehr bei der Entwicklung eines modernen, auf Software basierenden Funkgeräts sowie bei zukünftigen Funkstandards.

GSM, UMTS, LTE, WLAN, Bluetooth – Handys sind wahre Verbindungsgenies. Doch für jeden der genannten Funkstandards sind eigene Hard- und Software-Komponenten nötig. In Zukunft werden Mobiltelefone noch mehr Standards beherrschen und auf noch mehr verschiedenen Funkfrequenzen arbeiten. Damit der Aufwand nicht explodiert, haben die Ingenieure »Software Defined Radio« (SDR) erfunden. Die Idee: Die Hardware ist nicht auf bestimmte Funkstandards oder -frequenzen festgelegt, erst die Software entscheidet, welche Verbindungen das Gerät eingehen kann. SDR überträgt das Prinzip des Personal Computers, wo auf einer weitgehend standardisierten Hardware beliebige Software arbeitet, in die Welt des Funkverkehrs.

Diesen Weg will nun auch das Militär gehen. Dort sind Funkverfahren und -geräte im Einsatz, die oft schon 20 Jahre auf dem Buckel haben. Sie sind in erster Linie für Sprechfunk ausgelegt, eine gleichzeitige Übertragung von Daten ist nur eingeschränkt möglich. Künftig alle zwei Jahre neues Funkequipment zu kaufen, um auf dem neuesten Stand zu bleiben, wie wir Privatnutzer das bei Handy-Verträgen gewohnt sind, ist für militärische Anwender keine Alternative. Die Bundeswehr und die Streitkräfte anderer Nationen setzen deshalb auf Software Defined Radio. Damit soll der militärische Funkverkehr der Zukunft sicher, modular, programmierbar und rekonfigurierbar werden. Neue Standards oder Funktionen erfordern dann keine neuen Geräte mehr, sondern nur eine neue Software-Anwendung.

Lücken schließen

In Deutschland gibt es im Kontext des militärischen SDR vor allem zwei große Projekte. SVFuA (Streitkräftegemeinsame Verbundfähige Funkgeräteausstattung) beschäftigt sich seit 2008 mit der Entwicklung einer Hardware-Plattform. Vom Bundesministerium der Verteidigung haben mehrere Firmen – allen voran Rohde & Schwarz – den Auftrag erhalten, den Nachweis der Realisierbarkeit eines Software Defined Radios für militärische Zwecke zu erbringen. Die Partner entwickeln einen SDR-Prototyp, der zahlreiche Funkverfahren in einem weiten Frequenzbereich von 1,5 Megahertz bis 3 Gigahertz beherrscht.

Das Funkgerät schließt etliche Fähigkeitslücken. Sprache und Daten lassen sich künftig gleichzeitig übertragen, wie man das von Voice-over-IP-Telefonen oder von Skype kennt. Außerdem lassen sich damit mehrere Geräte ad hoc zu einem Netzwerk verknüpfen, bisher waren nur Punkt-zu-Punkt-Verbindungen oder Gruppenrundrufe möglich. Auch wird die Übertragungsgeschwindigkeit deutlich steigen, auf mindestens ein Megabit pro Sekunde. Das klingt bescheiden angesichts der Datenraten, die heute schon über WLAN-Knoten oder demnächst über den neuen Mobilfunkstandard LTE möglich sind. Allerdings sind die Voraussetzungen ganz andere. Der militärische Funkverkehr spielt sich bei weit


1

niedrigeren Frequenzen mit entsprechend geringerer Bandbreite ab. Außerdem muss er im Gegensatz zum Mobilfunk ohne feste Basisstationen auskommen, weil man nicht in jedem Einsatzgebiet in der Welt Mobilfunkmasten aufstellen kann, die obendrein erstes Ziel des Gegners wären.

Neben der SDR-Hardware kommt auch der Software, die die Funkverfahren realisiert, eine besondere Bedeutung zu. Ohne Software-Anwendungen ist das SDR-Gerät so wenig wert

wie ein Büro-PC ohne Windows und Office. Zwar werden in SVFuA einige der bisher genutzten Funkstandards als Software-Anwendungen auf das SDR-Gerät gebracht, aber damit lassen sich noch keine der neuen, gewünschten Fähigkeiten nutzen. Deshalb beschäftigt sich ein zweites Projekt namens COALWNW (Coalition Wideband Networking Waveform) mit der Entwicklung eines neuen Funkstandards, oder wie es im Fachjargon heißt: einer Wellenform. Dieser Begriff ist eigentlich irreführend, denn mit Wellenform ist keineswegs nur das bloße Aussehen von Funkwellen gemeint. Der Begriff umfasst vielmehr alle Datenverarbeitungsschritte etwa von der Spracheingabe im Mikrofon bis zur eigentlichen Signalübermittlung über elektromagnetische Wellen, auch Aspekte wie die Verschlüsselung sind darin enthalten. An COALWNW sind neun Nationen beteiligt, neben Deutschland, Großbritannien und Frankreich auch die USA. Die Kooperation soll sicherstellen, dass alle Partner am Ende dieselbe Wellenform benutzen und ein reibungsloser Datenaustausch bei internationalen Einsätzen möglich ist.

Gefragte Berater

Das Fraunhofer FKIE spielt sowohl bei SVFuA als auch in COALWNW eine zentrale Rolle. So ist Dr. Marc Adrat von der Abteilung Kommunikationssysteme des Fraunhofer FKIE der nationale Vertreter im virtuellen Projektbüro von COALWNW. Das SDR-Team am Fraunhofer FKIE berät das IT-Amt der Bundeswehr und vertritt es in technischen internationalen Arbeitsgruppen.

Die Forschungsaktivitäten am Institut zu Software Defined Radio dienen folglich nicht vorrangig der Entwicklung eigener SDR-Komponenten, sie sollen vielmehr helfen, die Beratungskompetenz der Experten sicherzustellen und auszubauen. So entwickelt das FKIE-Team Softwarelösungen für die aus dem SVFuA-Umfeld hervorgegangenen Geräte, um Lieferergebnisse der Industrie für das IT-Amt zu bewerten. Außerdem vergibt das Fraunhofer FKIE Forschungsaufträge an Partner: das Fraunhofer IIS in Erlangen, die Universität der Bundeswehr in München, das KIT in Karlsruhe und die RWTH Aachen.

Der Militärfunk stellt Anforderungen an die Sicherheit und Störresistenz, die weit über das im zivilen Funk Bekannte hinausgehen. Die Funkverbindungen, die mitunter viele Kilometer in unbekanntem Terrain überbrücken sollen, müssen zum Beispiel so ausgelegt sein, dass Dienste priorisiert werden können. So soll Sprache in der Regel Vorrang vor der Datenübertragung haben und es darf dabei zu keinen merkbaren Verzögerungen kommen. Wichtig für die Bundeswehr ist auch, dass sich die Hierarchie der Truppe in den Funknetzen abbilden lässt. Wenn die ersten Geräte mit Software Defined Radio in einigen Jahren in der Truppe eingeführt werden, sind diese vermutlich zunächst für den Betrieb in Fahrzeugen ausgelegt. Erst später wird es dann Endgeräte vergleichbar mit Handys geben, die dann aber aufgrund der kleineren Bauform nicht alle Frequenzbereiche abdecken können.

1/4 *Militärische Spezialisten arbeiten an der Harmonisierung ihrer unterschiedlichen Kommunikationssysteme.*
2 *Soldaten während einer multinationalen Großübung.*
3 *Soldaten beim Einrichten einer Satellitenverbindung.*

FELDTEST UNTER FREUNDEN

Combined Endeavor ist die weltgrößte Übung zur Interoperabilität von mobilen Kommunikationssystemen. Mit dabei: das Fraunhofer FKIE.

40 Nationen, 3000 Teilnehmer – das hat schon beinahe die Dimension von olympischen Spielen. Sportlicher Wettkampf stand indes nicht im Mittelpunkt der Veranstaltung, die vom 9. bis 22. September im pfälzischen Grafenwöhr stattfand. Auf dem Truppenübungsplatz trafen sich Soldaten zu Combined Endeavor 2011, um zu testen, wie gut der Datenaustausch zwischen den Nationen über mobile Funknetze klappt. Zwei Wissenschaftler des Fraunhofer FKIE waren ebenfalls mit dabei.

Von A wie Albanien bis V wie Vereinigte Staaten – jedes Land entscheidet frei, welche Hard- und Software es bei seiner Funkgeräteausrüstung einsetzen möchte. Das hat industriepolitische Gründe: Die Regierungen legen Wert darauf, wichtige Kompetenzen im Land zu halten und die eigenen Hersteller zu unterstützen. Doch das bereitet spätestens dann Probleme, wenn die Streitkräfte mehrerer Nationen in internationalen Einsätzen zusammenarbeiten müssen, wie derzeit in Afghanistan. Schon 1995 kam der Wunsch auf, die Kommunikationsverbindungen unter realen Bedingungen zu testen – Combined Endeavor war geboren. Seitdem findet die Übung jedes Jahr in Europa statt, 2010 zum ersten Mal in Grafenwöhr. Die Leitung der Übung lag wie auch in den Jahren zuvor beim Oberkommando der Streitkräfte der USA.

Kommunikation in der Krise

Die Teilnehmer spielen ein Szenario in vier fiktiven Missionsgebieten in Ostafrika durch. Die Trupps müssen Meldewege für Sprach-, Video- und Datenkommunikation nachbauen, auch unter erschwerten Bedingungen, etwa wenn die Lage in einem Krisengebiet eskaliert. Während der Fokus in früheren Jahren auf der technischen Umsetzung lag, hat sich das Interesse der Teilnehmer im vergangenen Jahr auf den Informationsfluss gerichtet, also auf die Frage, ob die Partner in Krisensituationen taktische Lageinformationen austauschen können.

Vor jeder Combined-Endeavor-Übung können Verbände der Bundeswehr ihren Testbedarf anmelden. Dieser wird mit den Partnern besprochen, die ihrerseits mitteilen, welche Ausrüstung sie zur Übung mitbringen. In regionalen Netzwerken besprechen die Länder, welche Pläne sie für die kommenden Jahre haben. Deutschland bildet ein regionales Netzwerk mit Finnland, Norwegen, Österreich und der Schweiz. In der Übung 2011 testete die Bundeswehr unter anderem das Führungsinformationssystem Heer sowie weitere Systeme etwa zur IP-Telefonie in einem Feldlager.

Bei Combined Endeavor geht es nicht allein darum, aktuelle Kommunikationsausrüstung zu testen, sondern auch künftige Entwicklungen voranzutreiben. Eine wichtige Rolle spielt hier TACOMS (Tactical Communication Standards for Joint Operations). Das Projekt wurde 2005 vom Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr aus der Taufe gehoben. Das Fraunhofer FKIE


1

bekam den Auftrag, eine Schnittstelle zum Datenaustausch zwischen den zehn Nationen zu entwickeln, die für ihre mobile militärische Kommunikation den Standard MobKommSys nutzen. Der vernetzt die IP-Telefone in verschiedenen Einsatzzentren untereinander über Satellit und Richtfunk.

Damit das auch ohne Vorplanung schnell und reibungslos klappt, wenn mehrere Nationen im Einsatz ihre Ausrüstung zusammenschalten, hat die NATO 2010 so genannte Interoperability Points festgelegt. Sie beschreiben den Übergang zwischen den Netzen

zweier TACOMS-Nationen. Die Vereinbarung definiert die vier unteren Netzwerkebenen, macht also verbindliche Vorgaben für Kabel und Stecker, IP-Adressierung, Routing sowie DNS (Domain Name Service). Alle anderen Informationen etwa von E-Mails, Videos oder Web-Dienstleistungen wie Lagebildern sind Standard-Internetdaten, die transparent über TACOMS weitergereicht werden. Für die IP-Telefonie wurde der Datenstandard H.323 festgelegt, der Übergabepunkt übersetzt die Daten jeweils in die nationalen Standards. Der Vorteil von TACOM: Die Eigenheiten der nationalen Systeme bleiben erhalten, dank der standardisierten Übergabepunkte klappt der Datenaustausch trotzdem.

Gelungene Verbindung

Die Ergebnisse von Combined Endeavor 2011 waren überwiegend positiv. Die TACOMS-Nationen Norwegen und Finnland ließen sich leicht über die Interoperability Points anbinden. Die Anbindung von nicht TACOMS-Nationen wie Aserbaidschan oder Belgien gelang ebenfalls und lief über »External Network Access Points«, die ebenfalls von der NATO festgelegt wurden und die militärische und zivile Standards berücksichtigen. »Allerdings war der Planungsaufwand relativ hoch«, resümiert Martin Lies, Leiter der Forschungsgruppe »Robuste heterogene Netzwerke« am Fraunhofer FKIE. Das Team berät die Bundeswehr und unterstützt sie bei der nationalen Planung der Übung. Die FKIE-Mitarbeiter sind außerdem Teil einer Technischen Arbeitsgruppe, die Technologievorausschau für die NATO betreibt und dafür sorgen soll, dass sich die mobilen Kommunikationssysteme der Nationen nicht auseinander entwickeln.

Ein Thema, das bisher bei TACOMS außen vor gelassen wurde, ist die Kryptographie. Wegen vieler nationaler Vorgaben konnten sich die Teilnehmer bisher nicht auf ein einheitliches Vorgehen bei diesem wichtigen Thema verständigen. »Dazu werden wir gesondert mit den Partnern sprechen«, sagt Martin Lies. Die Bedeutung von TACOM wird weiter steigen. Für Combined Endeavor 2012, das voraussichtlich wieder in Grafenwöhr stattfinden wird, haben sich bereits erheblich mehr MobKommSys-Trupps angemeldet als in früheren Jahren. Auch bei dieser Übung wird es nicht nur um reibungslose technische Kommunikation gehen, mindestens ebenso wichtig ist die Völkerverständigung. Hier dürfen sich die Teilnehmer erneut auf Sportturniere und Abendessen mit landestypischen Gerichten freuen.

1 Soldaten beim Aufbau und Einrichten einer Fernmeldestelle.
2 Die Flaggen der teilnehmenden Nationen.
3 Überprüfung der Fernmeldenetzplanung.

MASCHINE LIEST MIT

Ein Team von Computerlinguisten des Fraunhofer FKIE bringt Rechnern bei, Texte zu verstehen. Ihr Ziel: Datenbanken sollen bessere Informationen liefern.

»Ein primäres Amin ist Monoethanolamin, abgekürzt MEA.« Wenn Sie mit dieser Information nichts anfangen können, sind Sie in bester Gesellschaft. Wenn Sie allerdings in der Energieforschung tätig sind, könnte Sie dieser Satz interessieren. Vielleicht wollen Sie wissen, welche Methoden es zur Abscheidung von Kohlendioxid aus Kraftwerksabgasen gibt. Bei der Recherche werden Sie schnell auf Amine stoßen, denn diese binden CO_2. Wenn Sie den Begriff googeln, werden Sie jede Menge Treffer finden, doch welche Eigenschaften diese chemischen Verbindungen haben, wie sie in Kraftwerken eingesetzt werden und vor allem wer sich an Hochschulen und Forschungsinstituten mit dem Thema beschäftigt, werden Sie nur mit Mühe zusammensuchen können.

Besser wäre es, wenn man solche Inhalte über ein komfortables Informationssystem aus den Datenbanken abfragen könnte. Dieses Ziel hat EnArgus. In dem Projekt, das vom Bundesministerium für Wirtschaft und Technologie gefördert wird und bis 2013 läuft, bauen mehrere Fraunhofer-Institute, darunter auch das Fraunhofer FKIE, mit weiteren Partnern ein zentrales Informationssystem auf, das auf Forschungsvorhaben von Bund und Ländern aus dem Bereich der Energieforschung spezialisiert ist. Vor allem Mitarbeiter des Projektträgers Jülich, der in Deutschland große Teile der Energieforschung koordiniert, aber auch Abgeordnete oder Angehörige von Ministerien sowie interessierte Bürger sind potenzielle Anwender. »Welche Projekte werden in meinem Wahlkreis Lippe-Detmold zur Nutzung der Windenergie gefördert?« Solche Anfragen von Abgeordneten erforderten beim Projektträger Jülich bisher einigen Aufwand für die Recherche in etlichen Dokumenten. Künftig sollen unter Nutzung des EnArgus-Informationssystems solche Anfragen sehr viel effektiver bearbeitet werden können.

Wissen auf Knopfdruck

Dazu ist es aber notwendig, dass das Informationssystem nicht nur den Zugriff auf die Dokumente ermöglicht, sondern dass es in gewissem Maße auch semantisches Wissen parat hat, das den Nutzer bei seiner Anfrage unterstützt. Mit Wissen ist die Fähigkeit gemeint, Zusammenhänge zwischen Begriffen zu kennen. »Amine sind Absorptionsmittel.« Ein Experte sieht sofort den Zusammenhang zwischen diesem Satz und dem Satz oben. Eine Datenbank stellt diesen Zusammenhang nur her, wenn sie eine Ontologie enthält, die Konzepte der Energieforschung kennt und diese mit semantischen Relationen miteinander verknüpft. Eine einfache semantische Relation ist zum Beispiel die Hyponymie, die Über- und Unterbegriffe in Beziehung setzt. Im genannten Beispiel wären Amine ein Unterbegriff von Absorptionsmitteln. Für den Nutzer ist die Ontologie eine wichtige Unterstützung bei seiner Anfrage, weil sie ihm hilft, wichtige von unwichtigen Informationen zu unterscheiden.

Eine Ontologie von Hand zu erstellen ist enorm aufwändig. Es gibt zudem gar nicht genug Experten, die das erforderliche linguistische und das energiewirtschaftliche Fachwissen gleichermaßen beherrschen. Die Abteilung Informationstechnik für Führungssysteme des Fraunhofer FKIE nutzt deshalb ein computerlinguistisches Modul, das auf Vorarbeiten der Universität Sheffield basiert, um für EnArgus eine Ontologie zur Energieforschung zu erstellen. »Futter« für diese Ontologieerstellung sind Wiki-Texte, die die beteiligten Energieforschungseinrichtungen liefern. Die Wiki-Texte durchlaufen am Computer einen mehrstufigen Prozess der Informationsextraktion:

- Tokenizer: erkennt Wortgrenzen und Satzzeichen,
- Sentence Splitter: zerlegt den Text in Sätze,
- Part of Speech Tagger: weist Wortarten zu, generiert die Grundformen und erkennt morphologische Eigenschaften der Wörter,
- Named Entity Recognizer: erkennt Eigennamen und syntaktische Strukturen,
- Semantic Role Labeling: die Satzteile werden semantisch annotiert und ausgewertet,
- Ontology Builder: erweitert die vorliegende Ontologie.

Am Ende des Prozesses sind alle Wörter und Sätze mit ihren semantischen Eigenschaften bekannt. Im oben genannten Beispiel weiß das System nun, dass MEA eine alternative Bezeichnung von Monoethanolamin ist und dass es in die Oberklasse »Material« gehört und die Eigenschaften »porös« und »wasserlöslich« hat.

Interesse von großen Unternehmen

EnArgus ist nicht das erste und einzige Projekt, mit dem sich die Computerlinguisten im Team von Professor Ulrich Schade am Fraunhofer FKIE beschäftigen. Vorläufer war das Projekt AUGE. Es dient zur semantischen Suche in Texten, um militärische Bedrohungen zu entdecken. Quelle können Einträge der Soldaten in Führungsinformationssystemen sein, aber auch Zeitungsartikel, die im Einsatzgebiet erscheinen, oder Webseiten. Aktuell arbeitet das Team an weiteren Themendomänen, etwa zu Katastrophenschutz (Projekt CATO) und zu Smart Cities (Projekt EPIC). Interesse kommt neuerdings auch von Unternehmen, die große Textmengen – etwa Beschwerdemails von Kunden – vorsortieren wollen.

»NEUTRALITÄT UND UNABHÄNGIGKEIT BEWAHREN«

Dr. Michael Wunder ist Leiter der Abteilung Informationstechnik für Führungssysteme am Fraunhofer FKIE. Im Interview spricht der gelernte Maschinenbauingenieur über die Arbeit des Instituts in der Forschungsorganisation der NATO und erklärt, welchen Nutzen die Bundeswehr davon hat.

Wie hat sich die wehrtechnische Forschung in den letzten Jahren entwickelt?

Der Schwerpunkt hat sich von der eher langfristig angelegten, angewandten Grundlagenforschung – auch F&T-Stufe 1 genannt – zu eher anwendungsnahen Technologien – F&T-Stufe 2 – verschoben. In der Informations- und Kommunikationstechnik, mit der sich das Fraunhofer FKIE vor allem beschäftigt, werden damit Themen wie Abwehrmaßnahmen gegen IT-Bedrohungen – Stichwort: Cyber Defense – oder Anwendungen zur Entscheidungsunterstützung und zum Erzeugen relevanter Lageinformationen wichtiger. Der finanzielle und zeitliche Spielraum wird generell enger, das gilt auch für die wehrtechnische Forschung. Die muss deshalb verstärkt Kooperationspotenziale zur Zusammenarbeit mit der wehrtechnischen Industrie sowie anderen Wehrforschungseinrichtungen nutzen. Dabei wird das Fraunhofer FKIE in jedem Fall seine Neutralität und Unabhängigkeit von Marktinteressen bewahren, um die Bundeswehr vorurteilsfrei beraten zu können.

Welche Rolle spielt dabei die Research and Technology Organisation der NATO?

Die RTO ist ein wichtiges Forum für Forschung und Technologie in der Wehrtechnik. Sie ist in acht Panels & Taskgroups untergliedert, wobei das Information Systems Technology Panel für das Fraunhofer FKIE das Wichtigste ist. Rund 400 Wissenschaftler arbeiten im IST-Panel zusammen. Gemeinsam mit dem stimmberechtigten deutschen Vertreter aus dem Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr bin ich Mitglied im IST-Panel, in das alle an der NATO beteiligten Nationen Vertreter entsenden. Das Panel koordiniert die Aktivitäten von mehreren Research Technology Groups. In den RTGs wird die technische Sacharbeit geleistet. Meist etwa zehn bis fünfzehn Personen, darunter Wissenschaftler, Militärs und Industrievertreter aus einschlägigen Fachrichtungen, arbeiten dort für jeweils drei Jahre zusammen. Produkte oder Ergebnisse einer RTG sind insbesondere Demonstratoren, Symposien oder Workshops und natürlich ein umfangreicher Abschlussbericht, in dem die Erkenntnisse detailliert aufbereitet werden und der auch eine bewertete Übersicht über relevante Technologien beinhaltet.

Wieso ist die Arbeit in der RTO für das Fraunhofer FKIE so wertvoll?

Die RTO ist deshalb so attraktiv, weil die Spielregeln sehr einfach sind. Man muss nicht bei jedem Kooperationsprojekt ein Memorandum of Understanding unterzeichnen, da die RTO bereits den organisatorischen Rahmen bietet. Alle erarbeiteten Ergebnisse stehen grundsätzlich allen Partnern einer RTG zur Verfügung. Meist entsteht bei der Sacharbeit ein gewisses Vertrauensverhältnis, das die internationale Kooperation sehr fruchtbar macht. Und der Informationsaustausch in zahlreichen Arbeitsgruppen, Symposien und Workshops der RTO hilft einem, den Stand der eigenen Arbeit im internationalen Vergleich einzuschätzen.

Messen Sie sich dabei auch an der zivilen Forschung?

Die Universitäten haben traditionell gewisse Berührungsängste mit der wehrtechnischen Forschung. Andere politische Rahmenbedingungen, die die Kooperation von ziviler und wehrtechnischer Forschungsförderung fördern, haben in den letzten Jahren aber zu einer gegenseitigen Öffnung geführt, so dass unsere Verbindungen in die zivile Forschung inzwischen sehr gut sind. Durch die traditionell gleichen Interessen der in der RTO organisierten Wehrforscher bleibt sie natürlich für uns ein sehr wichtiges Forum.

Wie profitiert die Bundeswehr davon?

Im Rahmen unserer Grundfinanzierung durch die Bundeswehr sind Wissenschaftler des Fraunhofer FKIE in verschiedenen NATO-Gremien aktiv. Die dabei gewonnene Expertise, beispielsweise über die Schwerpunkte bei Forschung und Technologie in anderen Ländern, bringen wir auch in die F&T-Planungen der Bundeswehr ein. Darüber hinaus sprechen

wir technische Empfehlungen aus, bereiten Grundlagen für Standardisierungen vor und zeigen anhand von Demonstratoren, dass relevante Technologien für militärische Zwecke nutzbar sind. Das Fraunhofer FKIE übernimmt dabei zum Teil auch hoheitliche Aufgaben. Übrigens wurde das aktuelle Thema Software Defined Radio in einer RTG vorbereitet.

Grundsätzlich gilt, dass wir uns an Arbeitsgruppen in der RTO nur dann beteiligen, wenn wir auf dem entsprechenden Gebiet eigene Forschungsaktivitäten durchführen. Nur wenn man eigene Expertise einbringen kann, wird man von Partnern akzeptiert und nur dann funktioniert der gegenseitige Informationsaustausch.

Sind Sie auch auf Tagungen präsent?

Wir organisieren sogar mehrere. Ich durfte zum Beispiel Ende 2011 in Oslo ein IST-Symposium zu Semantischer Interoperabilität organisieren und leiten, an dem über 100 Experten und Mitglieder des IST-Panels teilnahmen. Die fachlichen Grundlagen für das Symposium wurden in einer RTG gelegt, die ich seit einigen Jahren leite. Kernthema ist, dass es beim Informationsaustausch zwischen Führungsinformationssystemen oft zu Missverständnissen – zu so genannten semantischen Brüchen – und in schwerwiegenden Fällen sogar zu Fehlentscheidungen und Kollateralschäden kommen kann.

Im kommenden Herbst organisieren wir in Koblenz eine Konferenz zum Thema Cyber Defense. Darüber hinaus sind wir beteiligt an zahlreichen weiteren Aktivitäten wie Specialists Meetings oder Lecture Series.

An welchen Projekten arbeitet Ihre Abteilung derzeit?

Ein aktuell wichtiges Thema ist das maschinelle Übersetzen selten gesprochener Sprachen. Wir arbeiten an Übersetzern für die in Afghanistan gesprochenen Sprachen Dari und Paschtu. Da es nur wenige vertrauenswürdige Dolmetscher gibt, hilft eine maschinelle Vorarbeit, die wenigen verfügbaren Kapazitäten zu entlasten. Aufgrund des sehr begrenzten Marktes hat die Industrie kaum Interesse an der Entwicklung entsprechender kommerzieller Produkte. Auch hier hat unsere Kooperation im Rahmen der RTO Vorteile, da wir uns die Arbeit mit anderen am Afghanistan-Einsatz beteiligten Nationen teilen können.

Ein großes Projekt, an dem das Fraunhofer FKIE beteiligt ist, ist die Harmonisierung der Führungsinformationssysteme der Bundeswehr. Alle Teilstreitkräfte haben bisher eigene, unterschiedliche Systeme. Ziel ist es, gemeinsam nutzbare Funktionalitäten zu etablieren und nur die tatsächlich notwendigen Spezialfunktionen individuell zu entwickeln. So lassen sich erhebliche Kosten sparen und die Interoperabilität verbessern. Das Projekt läuft über mehrere Jahre, in mehreren aufeinander folgenden Migrationsabschnitten werden Ergebnisse verfügbar sein. Das Fraunhofer FKIE unterstützt die Bundeswehr mit fachlicher Expertise, aber auch bei der Umsetzung und bei Koordinationsaufgaben.

Und mit welchen Themen wird sich Ihre Abteilung in Zukunft beschäftigen?

Ein Zukunftsthema ist die Anreicherung von Nutzinformationen durch Metainformationen. Dadurch lassen sich Hintergründe für einen Informationsaustausch wie Intention und Kontext für bessere Schnittstellen und auch für ein Wissensmanagement nutzen. Natürlich spielt auch die Mobilität von Anwendungen eine große Rolle. Durch die rasant gestiegene Leistungsfähigkeit von Smartphones und deren enorme Verbreitung durchdringt Informationstechnik mehr und mehr unseren Alltag, allgegenwärtige Computer werden Realität. Dadurch ergeben sich völlig neue Möglichkeiten für Führungsinformationssysteme und die spontane Interoperabilität beliebiger Nutzer.

KOMMUNIKATION OHNE HINDERNISSE

Das Fraunhofer FKIE testet, wie gut sich die Führungsinformationssysteme der NATO-Staaten untereinander verstehen.

Deutsch, Englisch, Französisch – in der NATO werden diese und noch viele weitere Sprachen gesprochen. Das macht die Kommunikation mitunter schwierig. Auch bei den Führungsinformationssystemen kommt es ab und zu zur Sprachverwirrung. Die Systeme, in denen Soldaten Lage- und Einsatzinformationen erfassen, sprechen eine Standard-»Sprache«, benutzen also ein einheitliches Datenformat und eine einheitliche Bedeutung für die verwendeten Begriffe – zumindest theoretisch. Doch die Entwickler der Systeme legen diese »Sprache« mitunter in unterschiedlichen Dialekten aus. Bei einem NATO-Einsatz kann das dazu führen, dass der Datenaustausch zwischen den Systemen ins Stocken gerät.

Solche Fallstricke zu erkennen und zu beseitigen ist das Ziel von CWIX (Coalition Warrior Interoperability Exercise). Die Übung findet jedes Jahr statt, 2011 im Joint Force Training Center der NATO im polnischen Bydgoszcz.

In einem zweiwöchigen Szenario, das einen UNO-Einsatz in zwei Fantasiestaaten am Horn von Afrika simulierte, prüften die Teilnehmer – meist ein Soldat sowie ein Informatiker – ihre Führungsinformationssysteme auf Herz und Nieren. Jede Nation entwickelt ihre eigenen Systeme, um die Entwicklungskompetenz im Land zu halten. Die Nationen verfügen in der Regel über mehrere Systeme. So besitzt die Bundeswehr für Heer, Marine und Luftwaffe unterschiedliche »FüInfoSys«.

Testsystem horcht mit

Auf dem Prüfstand steht bei CWIX für die Heeressysteme der MIP-Standard. Das »Multilateral Interoperability Programme« wurde – auch mit Hilfe des Fraunhofer FKIE – entwickelt, um den Datenaustausch zwischen den Führungsinformationssystemen zu gewährleisten. 29 Nationen haben sich MIP angeschlossen. Viele davon haben die neueste Spezifikation, MIP Baseline 3, bereits umgesetzt. Doch aus den CWIX-Übungen ist bekannt, dass es zu Kommunikationsproblemen kommen kann. So bereitet der Austausch von operationellen Informationen mit Hilfe des Datenmodells »Joint Consultation Command and Control Information Exchange Data Model« hin und wieder Schwierigkeiten.

Um diese Probleme systematisch zu untersuchen, wurde das Fraunhofer FKIE vom IT-Amt der Bundeswehr beauftragt, ein Testsystem zu entwickeln und damit die CWIX-Übung zu begleiten. Das Institut hat bereits öfters mit eigenen Systemen an der CWIX teilgenommen. 2010 nahm man zum ersten Mal mit dem Testsystem teil; in diesem Jahr wurde das Werkzeug noch einmal deutlich verfeinert. Das Testsystem zeichnet sämtlichen Datenverkehr während der Übung auf und prüft, ob der MIP-Standard eingehalten wird. Die Analyse geschieht auf mehreren Ebenen. So prüft das Testsystem, ob die Datenpakete syntaktisch und semantisch korrekt sind, aber auch ob die übermittelten Inhalte überhaupt sinnvolle Informationen enthalten.

Bei den Tests zeigte sich, dass sich die Umsetzung des MIP-Standards in etwa auf dem Vorjahresniveau befand. Keine Probleme gab es bei den Kommunikationsprotokollen. Das Verbinden und das Abonnieren von Informationen zwischen den verschiedenen nationalen Systemen klappte reibungslos, ebenso der Austausch einfacher Lageinformationen wie Ereignissen, Grenzen und Routen. Schwierigkeiten gab es hin und wieder bei der Übernahme der Daten in die eigene Datenbank, sodass manche Informationen nicht auf der Lagekarte dargestellt wurden. Umfangreiche Analysewerkzeuge zeichneten ein detailliertes Bild, welche Systeme welche Fehler begingen. Einige Fehler wurden von mehreren Systemen verursacht, ein Zeichen, dass der MIP-Standard im entsprechenden Bereich zu komplex ist. Die Erkenntnisse werden in einen zukünftigen MIP-Standard einfließen.

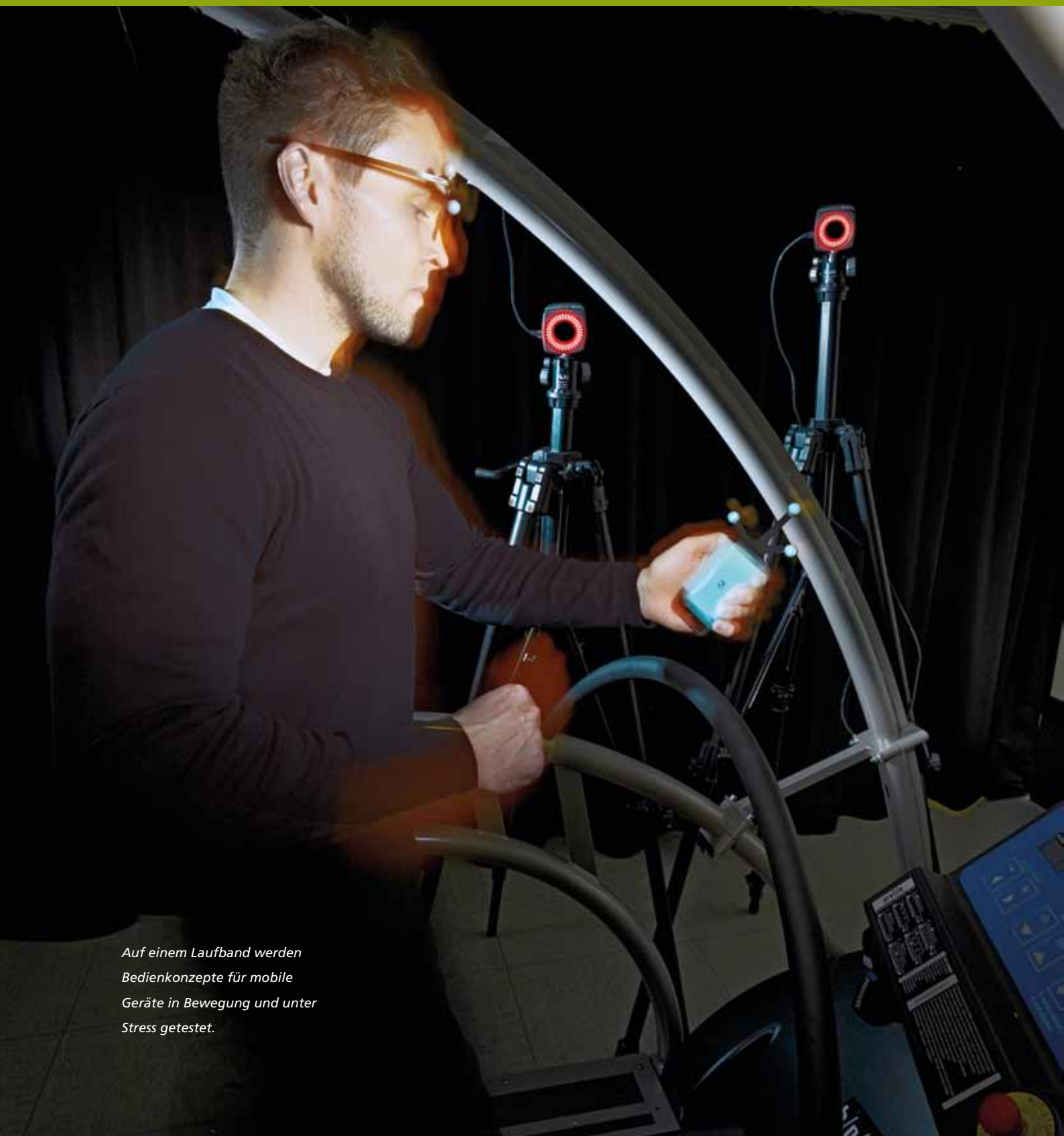
Konzentration auf das Wesentliche

Jeder kennt das: Software-Programme – etwa Textverarbeitungen – bieten viel mehr Funktionen, als man tatsächlich benötigt. Ob dies auch auf MIP zutrifft, untersuchte das Fraunhofer FKIE ebenfalls in der CWIX-Übung. Und tatsächlich: Der MIP-Standard ist so umfangreich und mit Funktionen überladen, dass weniger als ein Drittel der Funktionen im Laufe dieser Übung genutzt wurde. Intensiv verwendet wurden Informationen über Minenfelder oder Routen von Einheiten. Ungenutzt blieb dagegen zum Beispiel die Möglichkeit, für Aktionen die Ressourcen, Ziele oder gewünschten Effekte zu beschreiben. »Wir müssen uns bei MIP künftig auf das fokussieren, was wirklich benötigt wird«, fordert Dr. Michael Gerz, Leiter des CWIX-Teams am Fraunhofer FKIE. Aber die Grundfunktionen, die gebraucht werden, müssten dafür möglichst einfach und fehlerfrei umgesetzt werden.

Anstatt MIP mit immer neuen Funktionen aufzublähen, plädiert Dr. Gerz für den Umbau in einen modularen Standard. Das hätte viele Vorteile: Nicht jeder NATO-Partner müsste bei der Entwicklung seines Systems alle Funktionen auf einmal umsetzen. Vielmehr können sich die Streitkräfte auf die Funktionen beziehungsweise Module konzentrieren, die für sie wichtig sind. So muss das Heer in seinem Führungsinformationssystem nicht mehr die Kommunikationsbedürfnisse der Marine unterstützen. Das spart Zeit und Kosten, das Geld kann gezielter in die wirklich wichtigen Funktionen investiert werden.

EINGABE UNTER DRUCK

Wie müssen die Bedienoberflächen von kleinen mobilen Geräten wie Smartphones gestaltet sein, damit der Benutzer auch unter Stress damit zurecht kommt?



Auf einem Laufband werden Bedienkonzepte für mobile Geräte in Bewegung und unter Stress getestet.

Einfache Piktogramme erleichtern die Informationseingabe.

Ein Waldweg. Der Soldat läuft im strammen Marschtempo bergauf. Ein Kampfflugzeug donnert über die Wipfel, Vögel fliegen kreischend auf. Plötzlich erscheint am Wegesrand eine auffällige Person. Besteht Gefahr? Der Soldat tippt das Ereignis mittels einfacher Symbole in sein Smartphone, das die Lage an das Führungsinformationssystem übermittelt. Der Mann war friedlich, der Soldat eilt weiter durch den Wald.

»Stopp«, sagt Jessica Conradi. Das Fitnesslaufband hält an und die Testperson kann Atem holen. Der Waldweg verschwindet, und die Leiterin des Versuchs lädt eine neue Szene. Der Einsatz des Soldaten ist in Wahrheit eine Simulation in einem Labor der Abteilung Ergonomie und Mensch-Maschine-Systeme am Fraunhofer FKIE. Der Raum ist ausgestattet mit einem Laufband, einer riesigen Leinwand, Lautsprechern für den realistischen Sound und jede Menge weiterem Equipment wie Infrarot-Bewegungssensoren.

Die verblüffend realistische Szene auf der Leinwand stammt aus einem Spiele-Level, das die Forschungsgruppe Human Factors auf der Basis einer kommerziellen Spiele-Software entworfen hat. Diese Art der Verwendung von Spielen wird unter dem Begriff »Serious Gaming« zusammengefasst – die Vorteile und Eigenschaften der Spielsoftware werden genutzt, um sie fernab vom Spielen für wissenschaftliche Anwendungen zu nutzen. Es geht gar nicht um Kampfhandlungen, Conradi – Mitarbeiterin im Team Human Factors – ist an etwas ganz anderem interessiert: Sie möchte wissen, wie die Testperson unter Stress mit der Bedienung des Smartphones zurechtkommt. Stress wird auf der virtuellen Patrouille durch das plötzliche Auftauchen von Personen und Gegnern erzeugt, durch den Lärm der Kampfjets und durch die Sprachsignale, die der Proband in ein Headset sprechen muss. Stress entsteht aber auch, weil die Testperson nicht stehen bleiben kann. Das Fitnesslaufband läuft immer weiter – mit bis zu fünf Kilometer pro Stunde – und der Proband muss dabei die richtigen Symbole auf dem Touchscreen eingeben. Wer schon einmal versucht hat, beim zügigen Gehen eine SMS zu schreiben, kennt das Problem.

Zu viele Symbole

In dem Versuch geht es um ganz grundlegende Fragen: Wie sollten das Menü und die Benutzungsoberfläche strukturiert sein, damit man es im Laufen schnell und fehlerfrei bedienen kann, auch ohne dass man ständig die volle Aufmerksamkeit darauf lenkt? Soldaten verwenden taktische Zeichen, um sich einen Überblick über die aktuelle Lage zu verschaffen. Solche Zeichen könnten auch die Eingabe in das Smartphone erleichtern. Sie sind leicht zu erfassen und bei den Soldaten bekannt. Daher hat Jessica Conradi Symbole entwickelt, die vereinfachten taktischen Zeichen ähneln. Ab und zu erscheinen auf der Leinwand Quadrate und Kreise unterschiedlicher Form und Farbe und mit unterschiedlichen Rändern. Der Proband muss diese möglichst schnell eintippen.

Dass nicht zu viele Symbole gleichzeitig angezeigt werden können, sagt schon der gesunde Menschenverstand. Jedes einzelne Zeichen wäre viel zu klein und das Ganze zu unübersichtlich. Um herauszufinden, mit wie vielen Symbolen die Probanden zurechtkommen, wurden mehrere Varianten der Benutzerführung getestet. Bei Variante eins zeigt der Bildschirm nur zwei Grundsymbole und der Proband muss durch mehrfaches Tippen durch sechs Untermenüs die Bildattribute auswählen. Das andere Extrem ist eine Art Symboleditor, bei dem der Proband auf einer Ebene alle Merkmale bearbeiten kann und so das richtige Symbol erstellt. Das sieht schon ziemlich komplex aus. Auch Zwischenlösungen wurden ausprobiert, zum Beispiel mit vier Symbolen in drei Menüebenen oder acht Symbolen in zwei Menüebenen.

Wie häufig ist auch hier die goldene Mitte die beste Wahl. Vier Symbole sind auf dem Bildschirm noch gut zu treffen und durch drei Menüebenen tippt man sich flott durch. Auch acht Symbole gleichzeitig lieferten noch akzeptable Werte für die Fehlerhäufigkeit, die Häufigkeit der Blickabwendungen und die Zeit zur vollständigen Eingabe des Symbols. Überraschend: Das Lauftempo hatte keinen Einfluss auf die Eingabeleistung. Doch das könne auch an der sterilen Testumgebung liegen,

Die Benutzer müssen auch unter Stress Informationen schnell verarbeiten können.

meint Jessica Conradi. Das Labor hat zwar viele Vorteile, weil man eine Menge Faktoren vorbestimmen, kontrollieren und messen kann, auf die man draußen keinen Einfluss hat. Aber es ist eben nur fast wie draußen, vollständig kann man die Realität eben noch nicht simulieren. Entsprechend werden auch Außenexperimente folgen.

Die Untersuchung ist Teil einer Studie zur »Interaktion durch mobile Mensch-Computer-Interfaces für Führungssysteme« des Bundesamts für Wehrtechnik und Beschaffung. Hier wird aktuell daran gearbeitet, die Soldaten bei ihren Einsätzen durch die Ausrüstung am besten zu unterstützen und die Informationen der Soldaten im Feld in das Führungsinformationssystem der Bundeswehr einzubeziehen. Zukünftig wird der Infanterist viele elektronische Geräte mit sich führen. Zum Teil ist er schon heute mit elektronischem Kompass, GPS und Laserentfernungsmessgerät ausgestattet. Diese Geräte liefern viele Daten, die aber bisher nicht zusammengeführt und in das Führungsinformationssystem übermittelt werden. Doch die Position des Soldaten kombiniert mit der Richtung und Entfernung von Objekten wären wichtige Informationen für die Führungskräfte zur Lagebeurteilung. Um die Daten zu übermitteln, wird der Soldat ein Eingabegerät besitzen, das sich ähnlich wie ein Smartphone bedienen lässt. Um die Gestaltung solcher Geräte geht es in dem FKIE-Projekt.

Möglichst wenig Ablenkung

Vor dem Aufbau des virtuellen Einsatzes im Labor hat das FKIE-Team Soldaten befragt, die zum Teil auch in Afghanistan waren. In einem ersten Experiment testete Jessica Conradi, ob und welche Vorteile eine automatische Übermittlung von Daten für den Soldaten brächte. Klare Antwort: Ja. Wenn der Soldat durch einen Knopfdruck Informationen über Position und Peilung senden kann, ist das eine Erleichterung. Doch um zu übermitteln, um was für ein Objekt es sich handelt und ob es gefährlich ist, muss der Soldat zusätzliche Informationen eingeben. Und dafür ist das oben beschriebene Experiment gedacht. Conradi: »Die Erkenntnisse sind grundsätzlich überall dort interessant, wo Personen abgelenkt und unter Druck Eingaben in Geräte machen müssen.«

Das Projekt wurde 2011 abgeschlossen. In dem laufenden Folgeprojekt soll das Fraunhofer FKIE nun das Verhalten unter besonderer körperlicher Belastung studieren. Dazu wurde der Versuchsstand mit Infrarotkameras ausgerüstet. Sie zeichnen die Bewegungen der Testperson auf, die mit voller Ausrüstung auf dem Laufband unterwegs ist. Ebenfalls geplant ist ein Sehtest mit den durchbrochenen Ringen, die man vom Sehtest bei der Führerscheinprüfung kennt. In diesem Fall geht es aber um die Sehschärfe beziehungsweise um die Frage, ob und wie sich die Sehschärfe ändert, wenn die Testperson in Bewegung ist. Das hätte unter Umständen zur Folge, dass weniger und größere Symbole verwendet werden müssten. In den kommenden Monaten sind auch Tests im Freien geplant.

Die Ergebnisse gehen vom Auftraggeber an die Industrie, die damit möglichst bedienerfreundliche Geräte entwickeln soll. Design dürfe nicht vor Ergonomie gehen, fordert Jessica Conradi, »denn hier geht es schließlich um Leben und Tod.«

In virtuellen Umgebungen wird die Informationsdarstellung auf innovativen Displays getestet.

KURZER PROZESS

Der »Process Interviewer« des Fraunhofer FKIE erleichtert die Erfassung und Modellierung von Prozessen. Das hilft unter anderem beim Schutz von Verkehrsinfrastrukturen.

Wer macht was, wie und warum? Diese Fragen beantwortet eine Prozessanalyse. Viele Unternehmen nutzen solche Analysen, um Klarheit über Geschäfts- und Produktionsprozesse zu gewinnen und ihre Abläufe zu optimieren. Zur Prozessanalyse gibt es Software, mit der sich Abläufe erfassen, visualisieren und den Mitarbeitern vermitteln lassen. Alle Methoden der Prozessanalyse haben einen Nachteil: Der Analyst, der das Modell erstellt, und der Experte, der im Betrieb die Prozesse umsetzen muss, sind nicht ein und dieselbe Person. Dem einen fehlen die Einblicke in die technischen Abläufe, dem anderen fehlt das Prozessdenken. Schön wäre ein Werkzeug, mit dem die Experten, die tagtäglich in der Produktion oder am Ladentisch stehen, ihre Arbeitsabläufe selbst erfassen könnten. Auch dem Analysten würde es seine Arbeit erleichtern, wenn beide dieselbe Sprache sprechen. Bisher war das Wunschdenken, doch jetzt ist es Realität: Daniel Ley, Wissenschaftler am Fraunhofer FKIE, hat mit dem »Process Interviewer« ein Softwarewerkzeug entwickelt, das diese Kluft überbrückt.

Anstoß zum Process Interviewer gab das vom Fraunhofer FKIE koordinierte Verbundprojekt »Verbesserung der Sicherheit von Personen im Fährverkehr (VESPER)«, das vom Bundesministerium für Bildung und Forschung im Sicherheitsforschungsprogramm »Forschung für die zivile Sicherheit« der Bundesregierung gefördert wurde. Seit den Anschlägen vom 11. September 2001 gelten auch Fährschiffe als potenzielles Ziel terroristischer Anschläge. Wenn Fähren im Hafen liegen, gehen nicht nur Personen an und von Bord, auch Güter werden ein- und ausgeladen, Autos und LKWs fahren in den Bauch des Schiffs. VESPER, das 2011 beendet wurde, erzielte Fortschritte bei der Sicherheitsarchitektur und der Risikobewertung, außerdem wurden Sicherheits-Assistenzsysteme und ein Entscheidungsunterstützungssystem entworfen. Weil dazu erst die Kenntnis der Prozesse erforderlich ist, erfolgte auch eine Modellierung der Prozesse in Häfen und an Bord von Schiffen.

Automatisierte Interviews

Das Problem: Um die Prozesse zu erfassen, musste Daniel Ley mit Kollegen mehrmals nach Rostock und Lübeck fahren, wo er im Gespräch mit den Sicherheitsverantwortlichen am Hafen die Abläufe beim Be- und Entladen der Schiffe durchgesprochen hat. »Und während der Modellierung im Institut, kamen wieder neue Fragen auf«, erinnert sich Ley. Dieses wenig effiziente Hin und Her brachte ihn schließlich auf die Idee, die Interviews zu automatisieren – der Process Interviewer war geboren.

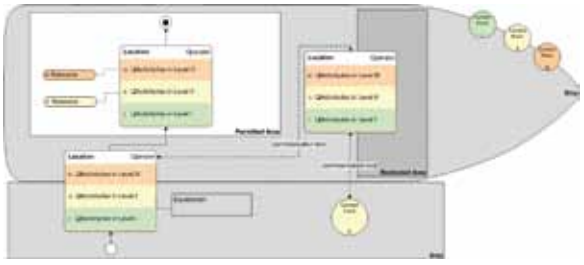
Das Programm bietet mehr als eine einfache Eingabemaske. Der Process Interviewer, der unter anderem auf der Modellierungstechnik K3 des Instituts für Arbeitswissenschaft der RWTH Aachen und der standardisierten Modellierungssprache für Geschäftsprozesse BPMN basiert, passt den Ablauf der Fragen vielmehr den Antworten an. Jeder Befragte durchläuft also eine individuelle Fragenreihenfolge. Am Ende des Interviews sind dennoch alle Fragen beantwortet – der Process Interviewer vergisst nichts. Die eigentliche Besonderheit ist aber ein zweites Fenster auf dem Bildschirm, das simultan zur Befragung ein Prozessdiagramm zeigt. Mit jeder Antwort verfeinert sich die Darstellung bis am Ende der komplette Prozess grafisch vorliegt.

Das hat mehrere Vorteile: Der Befragte sieht im Lauf des Interviews, wie der Prozess in Folge seiner Antworten Gestalt annimmt und kann eingreifen, wenn er Fehler im Prozessmodell entdeckt. Die Interaktion soll demnächst so weit gehen, dass der Befragte spielerisch mit dem Programm interagieren und selbst kreativ werden kann, etwa durch Verschieben von Prozessschritten mittels Fingerwischen auf einem Tabletcomputer. Unbewusst führt das zu einem Lerneffekt: Der Befragte versteht, wie die Abläufe seiner Arbeit zusammenhängen und er eignet sich ein prozessorientiertes Denken an, das ihm hilft, seine Arbeit besser zu planen und zu optimieren. Auch der Prozessanalyst, der die Auswertung übernimmt, profitiert: Er spart sich die aufwendige Umsetzung der Antworten in ein Prozessdiagramm, er kann gleich mit dem fertigen Diagramm weiterarbeiten. Daniel Ley hat festgestellt, dass der Process Interviewer die Zusammenarbeit zwischen Sicherheitsexperten und Prozessanalyst verbessert: »Beide sprechen jetzt dieselbe Sprache.«

2011 stellten Ley und sein Mitarbeiter, der die Programmierung durchführt, die erste Version vor, 2012 soll eine zweite, verbesserte Version folgen. Der Process Interviewer ist nicht nur für die Fährschifffahrt geeignet – im Prinzip lassen sich beliebige (Geschäfts-)Prozesse erfassen und modellieren. Anfragen gibt es auch aus dem eigenen Bereich, der Softwareergonomie. Profitieren würden insbesondere kleine Unternehmen, die bisher kein Geld für die Prozessoptimierung hatten. Daniel Ley sieht für den Process Interviewer großes Potenzial: »Es gibt meiner Kenntnis nach nichts Vergleichbares.«

SICHERHEIT AUF EINEN BLICK

Sicherheitsmaßnahmen in Häfen und an Bord von Schiffen sind komplex. Um die Übersicht zu behalten, hat das Fraunhofer FKIE in VESPER eine Methode zur Darstellung sicherheitsrelevanter Informationen entwickelt. SMT (*Security Modeling Technique*) zeigt Schiffe, Hafenanlagen und deren Schnittstellen mit farbigen Kästen, die für unterschiedliche Sicherheitsniveaus stehen, auch Maßnahmen, Prozesse und Kommunikationsketten werden abgebildet. SMT soll das Sicherheitspersonal in die Lage versetzen, Sicherheitsmodelle und die notwendigen Maßnahmen selbstständig zu entwickeln.



ALLES AUF EINE KARTE

Statt auf hoher See finden Marineübungen immer häufiger in Ausbildungszentren am Bildschirm statt. Das Fraunhofer FKIE hat ein besonders bedienerfreundliches Visualisierungswerkzeug für verteilte Simulationen entwickelt.

Administration einer verteilten Simulation mit VerSiA am Multi-Touch-Lagetisch.

Ein Bildschirm mit einer Karte von Europa. Beim Hineinzoomen sieht man mehrere Markierungen, die sich langsam durch die Nordsee bewegen. Die Piktogramme sehen aus wie kleine Schiffe – hier kreuzt also eine Flotte durch die virtuelle See. Etwas entfernt tauchen weitere Punkte auf, die wie Flugzeuge aussehen. Plötzlich löst sich eine Markierung, die auf eines der Schiffe zurast. Die Schiffe sind alarmiert und leiten Gegenmaßnahmen zum Abfangen des Objekts ein, bei dem es sich vermutlich um einen anfliegenden Flugkörper handelt.

Diesmal ist es nur eine Übung. Die deutsche Marine spielt häufig solche Szenarien durch, um für echte Bedrohungen gewappnet zu sein. Die gibt es in der Realität zuhauf, etwa in den aktuellen Einsätzen vor der Küste des Libanon oder am Horn von Afrika. Vor allem Einsätze, an denen verschiedene Teile der Streitkräfte beteiligt sind oder Verbände von Schiffen mehrerer Nationen, müssen immer wieder geübt werden, damit die Kooperation möglichst reibungslos klappt.

Die Übungen stammen aus einem Simulationswerkzeug, mit dem man Flottenmanöver erstaunlich realistisch nachbilden kann. Treibende Kraft hinter diesem Trend ist die US-Marine, die neue Schiffe in synthetischen Trainings zertifiziert. Die Überprüfung der Einsatzfähigkeit mittels Simulation spart Zeit und im Falle großer Flugzeugträger auch jede Menge Kosten. Für die Übungen kooperiert die US-Navy seit einigen Jahren mit den Flotten befreundeter Nationen. Die US-Marine liefert das »Drehbuch« für die Simulation, die anderen Nationen dienen als Sparringspartner.

Tücken der Technik

Bei der Deutschen Marine gibt es dazu den Taktischen Ausbildungs-, Unterstützungs- und Erprobungs-Systemverbund, kurz TAUES, der die technische Infrastruktur für Trainings, insbesondere für die Vernetzung der Simulation bereitstellt. Doch die technische Infrastruktur von TAUES hat Tücken: Sie besteht aus einer Vielzahl von Werkzeugen, die zum Teil inhaltliche Mängel haben und zudem unterschiedlichen Anzeige- und Bedienkonzepte verfolgen. Das schränkt die Effizienz der Übungen erheblich ein. Von der Bundeswehr kam der Wunsch, die verschiedenen Funktionen in einem intuitiv bedienbaren Simulationswerkzeug zusammenzufassen, das zudem Übungen in Eigenregie erlaubt, denn in den gemeinsamen Übungen mit der US-Marine haben die deutschen Partner keinen Einfluss auf den Ablauf der Trainings.

Hier setzt VerSiA (Verteilte-Simulations-Administration) an. Das Fraunhofer FKIE hat diese Software zur Steuerung verteilter Simulationen entwickelt, die Bundeswehr hat sie bereits gekauft und im Einsatz. VerSiA erfindet das Rad nicht neu, es setzt auf bewährte Standards, etwa auf DIS (Distributed Interactive Simulation). Auch Vorarbeiten anderer Abteilungen am Institut flossen ein, etwa das Lagebearbeitungssystem DIZZY der Abteilung Informationstechnik für Führungssysteme VerSiA kann über einen großen Touchscreentisch bedient werden. Was der Benutzer sieht, ist ein Lagebild wie in der Eingangsszene beschrieben. In der Karte kann er sich mit einfachen Gesten bewegen und in Details hineinzoomen. Piktogramme stehen für Schiffe, Flugzeuge und weitere Objekte. Mit Fingerwischgesten lässt sich zu jedem Objekt ein Kontextmenü öffnen, das Details zum Objekt wie Geschwindigkeit, Peilung oder Abstand preisgibt. VerSiA zeichnet alle Aktionen auf. Ist die Übung abgeschlossen, lässt sich der Ablauf mit den Teilnehmern im Debriefing noch einmal rekapitulieren.

Derzeit arbeitet die Marine bei synthetischen Übungen auch mit VerSiA noch auf herkömmlichen Laptops. Der Touchtisch kommt parallel erst einmal nur zu Testzwecken zum Einsatz. Die Evaluationen, die das FKIE-Team mit Anwendern zur Bedienerfreundlichkeit unternommen hat, sprechen aber klar für die innovative Touch-Lösung. »Die Interaktion mit der Software ist schneller und die Akzeptanz bei den Testpersonen war sehr hoch«, berichten Oliver Witt und Enrico Tappert, die mit ihren FKIE-Kollegen das VerSiA-Werkzeug entwickelt haben.

Trockenübung auf See

Zurzeit finden solche Simulationen auf dem Festland statt. Die Marinesoldaten sitzen in den Ausbildungszentren und üben an Rechnern. Das ist aber nicht besonders realitätsnah. »In Zukunft können die Operateure auf ihren Schiffen im Hafen bleiben und in ihrer gewohnten Umgebung üben«, verspricht Oliver Witt. Die Simulation würde dann zum Beispiel von der Ausbildungsleitung der Marine in Bremerhaven oder Wilhelmshaven gesteuert und an die teilnehmenden Schiffe am Pier verteilt. Ebenfalls geplant ist ein Szenariengenerator, mit dem der Administrator komplette Simulationen erstellen kann. Schon heute kann er das Lagebild verändern, zum Beispiel indem er mit einem Zeichenwerkzeug eine fiktive Insel in die Karte einfügt. VerSiA ist nicht allein auf Übungen der Marine beschränkt. Im Prinzip ist es für alle Arten von Simulationen geeignet, bei denen mehrere Akteure kooperieren und aufeinander reagieren müssen.

Kooperation von Teammitgliedern während eines synthetischen Trainings.

TREUER BEGLEITER

Das Fraunhofer FKIE hat eine Software entwickelt, die Personen zuverlässig erkennt und verfolgt. Der Tracker könnte einen Roboter steuern, der automatisch hinter einer Person herfährt.

Mensch oder Roboter – in vielen Einsatzgebieten gibt es eine klare Aufgabentrennung. Wenn es für Menschen zu anstrengend, zu schmutzig oder zu gefährlich wird, übernimmt die Maschine seine Vertretung, etwa beim Schweißen von Autokarosserien oder beim Bombenentschärfen. Doch es gibt viele Situationen, wo der Roboter als Partner Hilfestellung leisten könnte, wo also Mensch und Maschine ein gutes Team wären. Zum Beispiel bei militärischen Erkundungs- oder Kampfeinsätzen. Ein Roboter, der dem Soldaten im Feld auf dem Fuße folgt und Ausrüstung schleppt oder Aufklärung betreibt, wäre eine willkommene Erleichterung.

Das Projekt ARMINIUS (Assistenzfunktionen für Teilautonomie in mobilen unbemannten Systemen) des Bundesministeriums für Verteidigung untersucht genau solche Szenarien. Ziel ist es, den Soldaten in Zukunft durch Roboter zu unterstützen. Ein Thema dabei sind neuartige Bedienkonzepte. Der Soldat soll zum Beispiel einen selbstfahrenden Roboter, der sich in seiner Nähe befindet, ohne technische Eingabehilfen steuern können. Im Idealfall steuert sich der Roboter selbst, indem er automatisch einer Person folgt und ihre Gesten interpretiert. Damit der Roboter einer Person folgen kann, muss er diese erst einmal erkennen – eine hohe Hürde für bisherige Identifikationsalgorithmen. Die Forschungsgruppe Unbemannte Systeme des Fraunhofer FKIE hat nun in ARMINIUS ein Verfahren entwickelt, das sehr robust ist. Robust bedeutet: Der Algorithmus muss die Person zuverlässig verfolgen, bei schlechten Lichtverhältnissen ebenso wie wenn mehrere Personen durcheinanderlaufen und sich zeitweise verdecken. Und schließlich muss das Verfahren auch dann noch funktionieren, wenn der Roboter in hohem Tempo über Stock und Stein fährt und die Kamerabilder entsprechend verwackelt sind.

So sieht der Roboter die Szene. Die Rauten zeigen identifizierte Merkmale. Wird eine Person erkannt, weist ein grünes Rechteck darauf hin. Verdeckte Personen können nicht zuverlässig erkannt werden, worauf ein rotes Rechteck hinweist.

Das Erkennen, Identifizieren und Verfolgen von Personen ist für viele zukünftige Anwendungen von Robotern Voraussetzung. So auch für einen Roboter, der im Alltag Dinge für uns transportiert.

Training vor der Abfahrt

Bisherige Verfahren leisten dies nicht. Dort wird die zu verfolgende Person zunächst in einem Bild markiert und dann in den folgenden Bildern identifiziert. Dieser Ansatz erfordert ein so genanntes Bewegungsmodell. Das Programm muss also wissen, wie sich die Person typischerweise bewegt. Das funktioniert im Labor gut, in voller Fahrt jedoch gar nicht, weil sich die Erschütterungen des Roboter mit den Bewegungen der Person überlagern.

Anders der Tracker des Fraunhofer FKIE: Er nutzt einen Personendetektor, der vor der Abfahrt trainiert wird. Die Person stellt sich vor eine Kamera, dreht sich auch um, und die Software zieht aus den Bildern rund 60 Merkmale heraus, die für diese Person charakteristisch sind. Das kann die Silhouette sein oder das Gesicht, auch Muster auf der Kleidung berücksichtigt der Detektor. Für jede Person wählt der Detektor andere Merkmale, je nachdem, wodurch sich die Person äußerlich besonders auszeichnet. Hat die Person die Kleidung gewechselt, muss neu trainiert werden, doch das dauert nur Sekunden. Im Lauf der Zeit, wenn der Roboter die Person länger verfolgt, lernt der Algorithmus sie immer besser kennen und nimmt neue, geeignetere Merkmale hinzu und verwirft andere, zweideutige Merkmale, die sich nicht bewährt haben.

Der entscheidende Vorteil für den Einsatz auf fahrenden Robotern: Der FKIE-Tracker benötigt kein Bewegungsmodell. Auch wenn die Kamera wackelt und folglich die Merkmale der Person im Bild hin und her springen, findet der Tracker die Merkmale trotzdem sehr zuverlässig. Gefüttert mit verschiedenen Videos aus Alltagsszenen erzielt der Algorithmus eine Erkennungsrate von 80 Prozent – auch wenn die Person zeitweise verdeckt ist. Die Identifikation klappt sogar, wenn die Person von anderen, ähnlich gekleideten Personen verdeckt wird. Der Tracker kann sogar zwei Personen gleichzeitig verfolgen, die aneinander vorbeilaufen, ohne von der einen auf die andere, falsche Person zu springen.

Dass der Algorithmus tatsächlich in der Lage ist, einen autonomen Roboter zu steuern, haben Experimente des Fraunhofer FKIE mit einem Experimentalroboter bewiesen. Dieser war in der Lage, einer Person zu folgen, wenn er mit Fahrbefehlen aus dem Tracker gefüttert wird. Zehn Kamerabilder pro Sekunde reichen aus, um die Position einer Person ausreichend schnell schätzen zu können.

Kein Mensch vor lauter Bäumen

Der Personentracker ist ein wichtiger Schritt auf dem Weg zum Roboter als Partner des Soldaten. Weitere Schritte müssen folgen. Trotz der guten Ergebnisse muss der Tracker noch verbessert werden. Läuft die Person durch einen Wald, sieht der Tracker nach kurzer Zeit nur noch Bäume, die Person geht verloren. Hier könnten Wärmebildkameras helfen, die Mensch und Hintergrund auseinanderhalten, auch die Kombination mit 3D-Lasern, die dreidimensionale Bilder mit Tiefeninformation liefern, würde die Erkennungsrate verbessern. Solche Ergänzungen könnten gleichzeitig auch zur Gestenerkennung dienen – damit der Soldat ohne technische Hilfsmittel einfache Befehle wie »folgen« oder »stopp« erteilen kann. Microsofts Gestensensor Kinect für die Spielekonsole X-Box, der auch in der Wissenschaft immer häufiger zum Einsatz kommt, liefert gute Erkennungsraten nur in geschlossenen Räumen, wo die Infrarotsignale von den Wänden reflektiert werden. Im Freien wird der Sensor vom Infrarotlicht der Sonne irritiert.

Die Entwicklungsarbeiten in ARMINIUS sind auf die Unterstützung von Soldaten zugeschnitten. Dabei muss es aber nicht bleiben. Auch Serviceroboter, die einmal im Haushalt helfen oder kranke Menschen pflegen sollen, benötigen entsprechende Fähigkeiten. Interessant ist die Personenerkennung auch für die Automobilindustrie. Sie könnte helfen, Fußgänger auf der Fahrbahn zu erkennen und Unfälle zu verhindern.

MITTENDRIN STATT NUR DABEI

Eine Bildverarbeitungssoftware des Fraunhofer FKIE erkennt Oberflächen von Gegenständen im Raum. Das soll eines Tages die Orientierung ferngesteuerter Roboter erleichtern.

Das Gehirn des Menschen hat viele phänomenale Eigenschaften. Eine ist die Fähigkeit, Oberflächen von Gegenständen richtig zuzuordnen. Wir wissen, dass die große weiße Fläche eine Wand ist, die braune Fläche davor aber zu einem Schrank gehört. Unser Gehirn erkennt die Objekte und ihre Flächen sogar, wenn wir uns ein Auge zuhalten. Unser Gehirn ist so geschult, dass es Flächen und ihre Lage im Raum auch dann noch erkennt, wenn gar keine dreidimensionalen Informationen vorliegen.

Einsatzgebiet des Manipulatorroboters: Umgang mit gefährlichen Chemikalien.

Entnahme einer Wischprobe zur späteren Analyse.

Wie viel schwerer hat es da ein Computerprogramm. Aus der Kamera erhält es eine riesige Wolke aus Bildpunkten, denen man zunächst nicht ansieht, wo sie im Raum hingehören. Gehört ein Bildpunkt zu derselben Fläche wie der Bildpunkt daneben? Oder liegen die beiden Punkte in Wirklichkeit einen halben Meter in der Tiefe versetzt? Was unser Gehirn in Sekundenbruchteilen löst, fällt Bildalgorithmen extrem schwer.

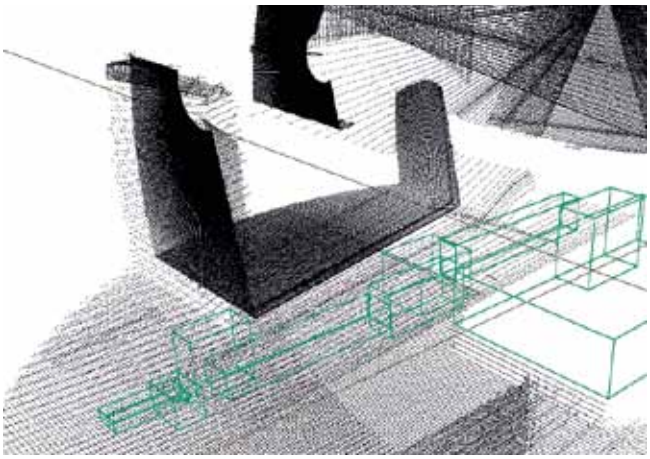
Auch die Forschungsgruppe Unbemannte Systeme des Fraunhofer FKIE kann keinen Algorithmus programmieren, der es mit einem Gehirn aufnimmt. Dennoch hat das Team in den letzten zwei Jahren einige Fortschritte erzielt, wenn es darum geht, in Bilddaten Flächen und Objekte zu erkennen. Die Entwicklung ist Teil von ManiPuR. In dem Projekt entwickelt das Fraunhofer FKIE einen mobilen Roboter mit Manipulatorarm. Der soll in Situationen, in denen möglicherweise biologische, chemische oder radioaktive Kampfstoffe eingesetzt wurden, Wischproben entnehmen. Der Soldat befindet sich dabei in sicherer Entfernung und steuert den Roboter und Arm mit dem Probennehmer.

Punkte zu Ebenen

Trotz Bildkontakt ist das aber gar nicht so einfach. Denn wenn eine Kamera (oder ein Laserscanner) und ein Monitor das Bild übermitteln, ist es mit der traumwandlerischen Orientierung unseres Gehirns nicht mehr weit her. Zwar erkennt es eine Wand oder einen Schrank, doch wie weit sie tatsächlich entfernt sind, ist auf dem zweidimensionalen Bildschirm schwer zu erkennen. Steuert der Soldat den Manipulatorarm aus der Ferne mittels Joystick, wird der Arm öfters ungestüm gegen Hindernisse stoßen. Doch bei der Entnahme biologischer Proben kommt es auf Fingerspitzengefühl an, wenige Millimeter können entscheiden, ob eine Probe erfolgreich war oder ob das Objekt beschädigt wurde.

Was der steuernden Person bisher fehlte, ist ein räumlicher Eindruck der Szene und eine Vorstellung, wie Objekte im Raum orientiert sind. In seiner Diplomarbeit an der Universität Bonn hat Bastian Gaspers für das Fraunhofer FKIE ein Verfahren entwickelt, das genau dies leistet. Es nutzt die Bilddaten eines Laserentfernungsmessers. Der ist auf dem Manipulatorarm montiert und wird herumgeschwenkt, wobei er zu jedem Objektpunkt die Entfernung misst. So entsteht eine dreidimensionale Punktewolke. In seiner Arbeit hat Gaspers zwei Verfahren – die Hough-Transformation sowie den RANSAC-Algorithmus – kombiniert, um Ebenensegmente aus der Punktwolke zu extrahieren.

Das Verfahren geht mehrskalig vor. Erst sucht es in der Punktwolke mit einem groben Raster nach Punkten, die zu einer Oberfläche gehören. Dann wird die Auflösung verfeinert, wodurch weitere Punkte zu kleineren Oberflächen verbunden werden. So geht das weiter bis zur feinsten Auflösung, wo die Zuordnung aller Punkte noch einmal überarbeitet und endgültig festgelegt wird. Die Strategie »von grob nach fein« hat den Vorteil, dass die Datenmenge rasch schrumpft, die meisten



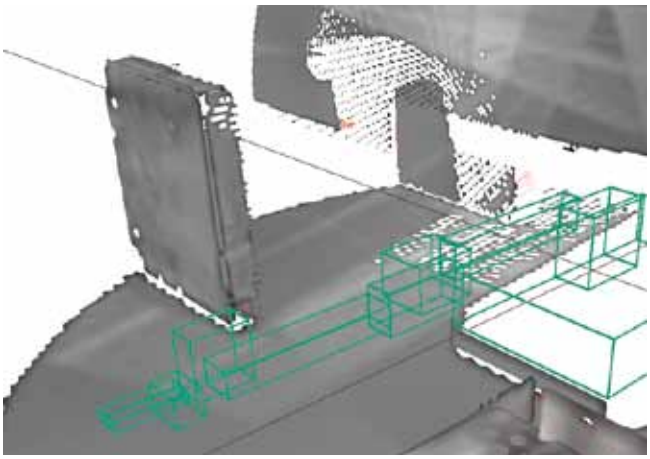
Eingabepunktwolke mit eingeblendetem Manipulatorarm.

Ebenensegmente werden schon in der groben Auflösung gefunden. Das Verfahren arbeitet mit unsortierten Punktwolken, funktioniert also sowohl mit Laserentfernungsmessern als auch mit Daten aus 3D-Kameras oder der Infrarot-Gestensteuerung Kinect von Microsoft. Wird die Kinect eingesetzt, liefert sie außerdem die Farben der Oberflächen.

Nachträglich bunt

Bastian Gaspers hat das Verfahren auf der International Conference on Intelligent Robotics and Applications 2011 mit Erfolg vorgestellt. Als nächstes will er Farbinformationen auch ohne Kinect, also nur mit dem Laserscanner auf dem Manipulatorarm, ins Bild einfügen. Die Software weist dann jeder zusammenhängenden Fläche eine gemeinsame Farbe zu. Außerdem ist geplant, auch kompliziertere Oberflächen etwa von Zylindern, Kegeln oder Kugeln zu erkennen. »In Zukunft wird es vielleicht sogar möglich sein, Objekte wie »Tisch« oder »Baum« zu klassifizieren«, hofft Bastian Gaspers.

Was hat der Benutzer von alledem? Er wird eines Tages einen Roboter fernsteuern und dabei viel besser einschätzen können, wo sich Objekte in einem Raum befinden, den er nur durch die Augen der Kamera oder eines Laserscanners sehen kann. Der Benutzer wird die Szene am Monitor drehen und quasi hinter Gegenstände schauen können. Zusammen mit anderen Arbeitspaketen des ManipuR-Projekts wird es dann möglich sein, Bewegungen des Manipulatorarms automatisch zu planen.



Darstellung der detektierten Ebenen.

Segmentierte Punktewolke einer Büroszene mit einem Karton im Vordergrund. Die Farben kodieren die Ebenenzuordnung.

DER GEFAHR BEWUSST

Was tun bei einem Cyber-Angriff? Ein intuitives Lagebild erleichtert die Einschätzung der Situation und das Ergreifen von Gegenmaßnahmen.

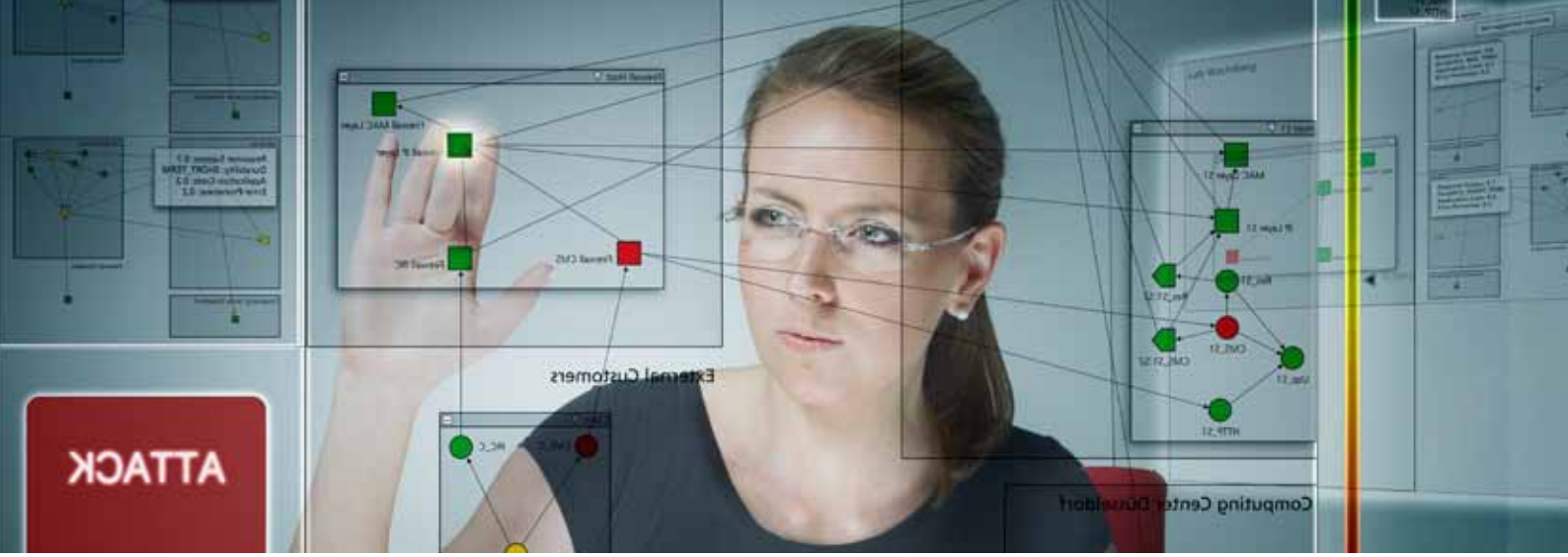
Der Online-Shop eines großen Versandhändlers. Kunden bleiben mitten im Einkaufsprozess stecken, so als sei der Browser ihres Computers abgestürzt. Innerhalb weniger Minuten geht im Online-Shop nichts mehr. Wenn nicht schnell etwas geschieht, werden viele Kunden ihren Einkauf abbrechen und der Anbieter verliert einen erheblichen Teil des Tagesumsatzes. Ein Experte des zuständigen Security-Operations-Center tippt auf den großen Touchscreen, um der Ursache auf den Grund zu gehen. Rote Punkte in der Box, die für das Internet steht, verheißen nichts Gutes. Kein Zugriff von externen Browsern, sogar der Administrator hat keinen Zugang mehr auf den Online-Shop. Die Ursache ist schnell gefunden. Der Server, auf dem die Shop-Software läuft, ist ebenfalls rot markiert; er ist das Ende in der betroffenen Kette. Ein Tipp auf das Kontextmenü zeigt Detailinformationen, die den Schluss nahelegen, dass hier gerade ein Denial-of-Service-Angriff läuft. Ein Saboteur bombardiert mit »Zombie«-Rechnern, die er unter seine Kontrolle gebracht hat, den Online-Shop mit Dienstanfragen und verhindert, dass Kunden den Shop erreichen können. Mit wenigen weiteren Fingergesten wählt der Sicherheitsexperte einige angemessene Maßnahmen zur Rekonfiguration von Netz und Serversystemen aus und aktiviert zusätzliche Ressourcen. Nach kurzer Zeit sind die Auswirkungen der Maßnahmen im Lagebild sichtbar: Die Server sind zwar immer noch stark belastet doch der Verkauf kann erst mal weitergehen.

Solche DoS-Angriffe sind leider an der Tagesordnung. Dass der Angriff diesmal keinen Schaden anrichtete, hat zwei Gründe: Erstens handelte es sich nur um eine Simulation im Labor des Fraunhofer FKIE und zweitens hat das Team der Forschungsgruppe Cyber Defense mit der interaktiven IT-Sicherheitslagedarstellung ein Werkzeug entwickelt, das künftige Angriffe effektiver beherrschbar macht. In dem Projekt geht es nicht nur um die Entwicklung einer intuitiven Benutzeroberfläche für einen Touchscreen. Hier setzt das Team auf die Vorarbeiten anderer Abteilungen des Fraunhofer FKIE auf, etwa auf die Lagebilddarstellung für die Marine zum Schutz der Schiffe vor feindlichen Angriffen, die in der Abteilung Ergonomie und Mensch-Maschine-Systeme entwickelt wurde. Wichtiger Unterschied: Bei der Marine ist der Raum ein Gewässer und damit real, das Cyber-Lagebild bildet dagegen Rechnernetze und damit einen virtuellen Raum ab. Eigentliche Aufgabe des Lage-Analysators ist vielmehr die Schärfung des Situationsbewusstseins. Der Experte, der den Angriff abwehren muss, soll von der Informationsflut entlastet und so mit Gefahreneinschätzungen und Handlungsalternativen versorgt werden, dass er schneller die richtigen Entscheidungen treffen kann.

Software erleichtert Entscheidung

Das Konzept, das dem Projekt m-CDSA (Model-based Cyber Defense Situational Awareness) zugrunde liegt, stammt aus der Kognitionswissenschaft. Situationsbewusstsein bezeichnet die Fähigkeit, Objekte in der Umgebung zu beobachten, ihr Verhalten zu verstehen und eine Vorhersage über ihr Verhalten in naher Zukunft treffen zu können. Dieses Konzept lässt sich auf Cyber Defense – den Schutz kritischer Rechnernetze – übertragen. Doch das Beobachten, Verstehen und Vorhersagen ist hier gar nicht so leicht. Herkömmliche Software-Werkzeuge liefern riesige Mengen von schwer interpretierbaren Meldungen, aus denen der Sicherheitsexperte Bedrohungen der IT-Infrastruktur eines Unternehmens oder einer Behörde herauslesen muss. Das führt zu einer kognitiven Überlast, auch wenn der Experte ein tiefgehendes technisches Verständnis der zu schützenden Systeme und der Fähigkeiten des Angreifers hat. Doch das kann man in der Praxis nicht immer voraussetzen. Das Modell von der Wirklichkeit, das der Analyst in seinem Bewusstsein erstellt, ist deshalb häufig lückenhaft. Er übersieht Abhängigkeiten zwischen kritischen Systemen, was zur Auswahl einer falschen Handlungsalternative und zu Kollateralschäden im eigenen Netz führen kann. Ziel von m-CDSA ist es, die Bildung dieses mentalen Modells durch Software zu unterstützen und damit die Entscheidungsfindung zu erleichtern.

Um verlässliche Entscheidungen zu treffen, sind viele Daten aus verschiedenen Quellen nötig. Diese umfassen unterschiedliche Werkzeuge der IT-Sicherheit, etwa Virenprüfprogramme, die E-Mails und Daten auf Rechnersystemen untersuchen oder



Intrusion-Detection-Systeme, die den Netzverkehr überwachen und auf Anzeichen für Angriffe oder Abweichungen von einem zuvor erlernten Normalverhalten überprüfen. Solche Werkzeuge gibt es schon länger, doch sie betrachten immer nur einen Ausschnitt der gesamten Bedrohungslage. Eine ganzheitliche Übersicht der Meldungen und ihre intuitive Darstellung, die exakt für die Bedürfnisse der IT-Sicherheitslage zugeschnitten sind, gab es bisher nicht. Hier soll das FKIE-Projekt Abhilfe schaffen.

Nachhaltiger Schutz

Das Cyber-Lagebild soll keine Experten aus Fleisch und Blut ersetzen – diese treffen immer die letzte Entscheidung. Es soll vielmehr alle relevanten Informationen zusammentragen, durch entsprechendes Hintergrundwissen ergänzen und so aufbereiten, dass der Sicherheitsanalyst in der Lagezentrale die bestmögliche Entscheidung treffen kann. Diese ist von vielen Faktoren abhängig. So ist bei einem DoS-Angriff etwa auf einen Online-Shop die für die eigenen Ressourcen schonendste Lösung – nämlich das zeitweise Abschalten der betroffenen Server – für das Unternehmen nicht unbedingt die beste, weil dadurch Umsatz verloren geht.

Das Cyber-Defense-Lagebild des Fraunhofer FKIE liefert deshalb Handlungsempfehlungen, die auch nachhaltig Sinn ergeben. Sie berücksichtigen die aktuellen Prioritäten des Unternehmens und kalkulieren vor diesem Hintergrund die zu erwartenden Kosten von Reaktionsmaßnahmen und stellen sie dem zu erwartenden Reaktionserfolg gegenüber – etwa in welchem Maß die Server-Erreichbarkeit wieder hergestellt wird. Daraus lässt sich auch ableiten, wie sich solche Angriffe künftig vorher verhindern lassen. Das Projekt m-CDSA wird derzeit aus Anschubmitteln des Bundesministeriums für Verteidigung finanziert. Es zeigt interaktiv die Möglichkeiten der entwickelten Lösung und ist damit eine wichtige Vorlaufforschung für die konkrete Umsetzung beim Kunden. Die Darstellung der IT-Sicherheitslage ist in vielen öffentlichen und kommerziellen Bereichen von wachsender Bedeutung, das Projekt hat damit für die Forschungsgruppe Cyber Defense und für das Institut eine strategisch wichtige Rolle. Verschiedene Unternehmen haben bereits Interesse an der maßgeschneiderten grafischen Aufbereitung der Cyber-Lage bekundet, ebenso Bundeswehr, Polizei und andere Behörden.

Ein m-CDSA-Lagebild verschafft den Experten einen Überblick und liefert Handlungsempfehlungen im Bedrohungsfall.

STRATEGIEN GEGEN CYBER-ATTACKEN

Viren und Spam-Mails sind die Plagen des Computerzeitalters. Weit gefährlicher sind allerdings Botnetze – gekaperte und vernetzte Rechner, die Cyberkriminelle für massive Angriffe gegen Unternehmen oder Behörden einsetzen. Das Fraunhofer FKIE arbeitet an der Analyse und Abwehr solcher Attacken und berät Behörden und Unternehmen, welche Gegenmaßnahmen sinnvoll sind.

Windows, Office und ein guter Virenscanner – das ist die Grundausstattung der meisten PCs. Dass eine Software zur Abwehr von Angriffen aus dem Internet unbedingt notwendig ist, hat sich herumgesprochen. Damit ist das Problem aber nicht gelöst, denn auch die Gegenseite rüstet auf – die Bedrohung hat in den letzten Jahren deutlich zugenommen. Symantec, ein Anbieter von Sicherheitssoftware, beziffert den weltweiten Schaden durch Cyberattacken in 2011 auf 388 Milliarden Dollar, ein knappes Zehntel davon – 33,8 Milliarden Dollar – in Deutschland. Der Trend geht dabei weg von schrotschussartigen Massenangriffen auf beliebige Rechner hin zu gezielten Angriffen von Profis auf Computernetze mit besonders wertvollen Informationen.

Professionelle Angriffe erfordern professionelle Abwehrmaßnahmen. Seit zehn Jahren beschäftigt sich das Fraunhofer FKIE zunehmend mit Bedrohungen von IT-Infrastrukturen, gebündelt wurden die Aktivitäten 2010 in der Forschungsgruppe Cyber Defense. Sie betreibt das Cyber Defense Lab: Dort überwacht das Team Infrastrukturen und schlägt Alarm, wenn neue Schädlinge eindringen, es analysiert Botnetz- und Malware-Attacken unter Realbedingungen und entwickelt Abwehrmechanismen wie kryptografische Verfahren. Großen Wert legen die Mitarbeiter auf die verständliche Aufbereitung der Bedrohungslage für die Kunden, denn abstrakte Fehlermeldungen fördern nicht gerade das Problembewusstsein. Hier zahlt sich die interdisziplinäre Vernetzung im Institut mit Experten für Ergonomie und Mensch-Maschine-Schnittstellen aus. Auf Wunsch berät und schult die Forschungsgruppe Kunden zum Thema IT-Sicherheit.

Ein wichtiger Auftraggeber des Fraunhofer FKIE im Themenbereich Cyber Defense ist das Bundesamt für Sicherheit in der Informationstechnik in Bonn, für viele weitere Behörden und Unternehmen ist das Institut erster Ansprechpartner beim Thema IT-Sicherheit. Dort besteht Nachholbedarf: Nur 28 Prozent der deutschen Firmen arbeiten beim Schutz ihrer Infrastrukturen mit staatlichen Stellen zusammen. Das Fraunhofer FKIE versteht sich hier als Beratungsstelle, die Wissen zu IT-Sicherheit erarbeitet und zur Verfügung stellt.

Schweizer Taschenmesser

Ein Arbeitsschwerpunkt der Forschungsgruppe sind Botnetze – eine noch recht neue Bedrohung. Botnetze – ein Kunstwort aus Roboter und Netz – gelten als »Schweizer Taschenmesser« der Cyber-Kriminellen. Darunter versteht man gekaperte Rechner, die gemeinsam dank der zunehmenden Verbreitung von Breitband-Internetanschlüssen schwere Angriffe fahren können, zum Beispiel DDoS-Attacken, wobei DDoS für Distributed Denial of Service steht. Dabei wird der Rechner des Opfers so mit Anfragen überschwemmt, dass dieser den normalen Zugriff für Kunden des Betreibers verweigert. Häufige Angriffsziele sind Behörden oder Unternehmen, die den Zorn von Bürgern oder enttäuschten Kunden auf sich gezogen haben oder die Internetdienste als vorwiegendes Geschäftsprinzip einsetzen. Außer zu Rachefeldzügen lassen sich Botnetze zum Ausspähen von Kreditkartendaten nutzen. Immer häufiger dienen sie auch als Druckmittel, um Geld von Unternehmen zu erpressen.

DDoS-Angriffe sind besonders effektiv, wenn möglichst viele gekaperte Rechner dafür eingespannt werden können. Ein weiteres Beispiel sind Spam-Mails. Erst Botnetze haben den Massenversand von Werbemails oder virenverseuchten Nachrichten zum lukrativen Geschäft gemacht. Was Botnetze so gefährlich macht: Im Gegensatz zu Viren und Trojanern sind sie nicht nur für einen Angriffszweck ausgelegt, sondern lassen sich immer wieder neu konfigurieren und für verschiedene

Angriffe missbrauchen. Gleichzeitig liefern sie enorme Rechenkraft und eine große Bandbreite zu geringen Preisen. Eine Stunde DDoS-Angriff gibt es für zehn Dollar, der Versand von fünf Millionen Spam-Mails kostet 300 Dollar, berichtet der US-Reporter Brain Krebs. Angeboten werden die kriminellen Dienste über das Internet, auch über soziale Netzwerke wie Facebook.

Studie zu Botnetzen

Für die Europäische Agentur für Netz- und Informationssicherheit hat das Fraunhofer FKIE ein Projekt zum aktuellen Stand der Abwehr von Botnetzen ausgeführt. Die Studie »Botnetze: Erfassung, Messung, Desinfektion und Abwehr« gibt neben technischen Empfehlungen auch Hinweise auf rechtliche Maßnahmen im europäischen Kontext. Ein separater Bericht mit dem Titel »Botnetze: Zehn knifflige Fragen« liefert politischen Entscheidungsträgern Informationen zum Kampf gegen solche Angriffe.

Ein Thema, das die Sicherheitsexperten des Fraunhofer FKIE derzeit umtreibt, ist das Cloud-Computing. Immer mehr Dienste verlagern sich ins Netz in die »Wolke«, weil Online-Verbindungen heute fast so schnell sind wie der Zugriff auf die Festplatte im eigenen PC. In vielleicht zehn Jahren, so die Prognose, laufen die meisten Programme nicht mehr auf dem PC, sondern in zentralen Rechenzentren im Internet, abgespeckte PCs dienen dann nur noch als Internetterminal. Aus Sicht der IT-Sicherheit hat das Vor- und Nachteile. Beim Cloud-Computing muss sich nicht mehr der Nutzer um den Schutz seiner Daten kümmern, sondern der Anbieter des Cloud-Dienstes. Das macht Cloud-Computing für große Unternehmen und Behörden interessant, die für ihre IT-Sicherheit großen Aufwand treiben müssen. Der Nachteil ist, dass enorme Datenmengen von Millionen Nutzern an einem Ort gespeichert sind. Das macht diese Rechenzentren zu einem besonders verlockenden Angriffsziel. Auch wenn die Sicherheitshürden sehr hoch sind – wenn der Angriff gelingt, ist der Nutzen für den Angreifer groß und der Schaden für den Betreiber des Dienstes und seine Kunden verheerend. Das Cyber Defense Lab überwacht mit automatisierten Systemen die Infrastrukturen seiner Kunden. Angriffe lassen sich dadurch schon im Keim ersticken.

Honigtopf als Lockmittel

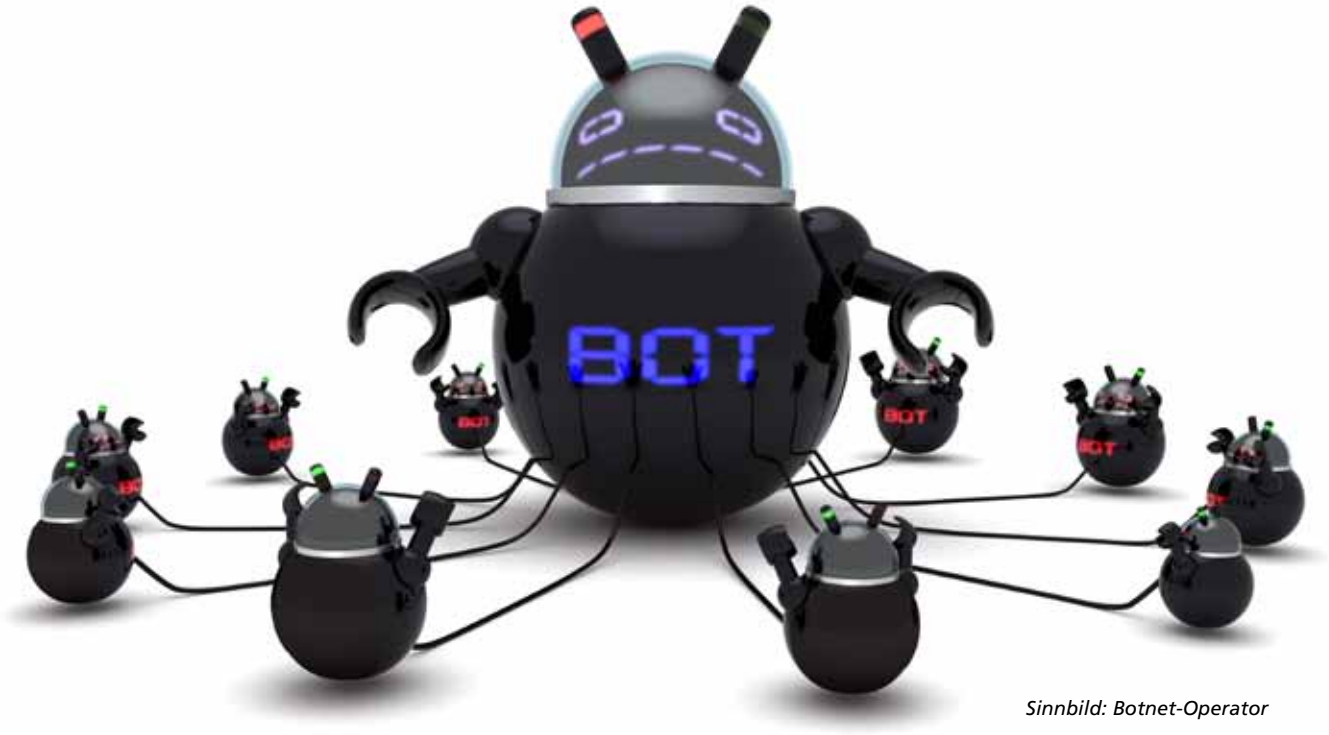
Eine simple Strategie, um Angreifern auf die Schliche zu kommen, geht auf den britischen Autor Alan Milne zurück. In einer seiner Kindergeschichten schreibt er, wie der etwas einfältige Bär Winnie Pooh mit einem Honigtopf gefangen wird. Auch in der Cyber-Abwehr gibt es so genannte Honeypots, die Angreifer anlocken sollen. Die Schadprogramme richten im Honigtopf keinen Schaden an, können aber analysiert werden, so dass künftige Angriffe leichter zu parieren sind. Das Fraunhofer FKIE geht einen Schritt weiter: Statt nur die Daten eines Honeypot zu sammeln, bauen die Fraunhofer-Forscher ein kooperatives Honeynet, in dem Honeypots Informationen austauschen und automatisch aufbereiten.

Gegen Viren, die Krankheiten auslösen, helfen meist Impfungen. Ähnliches versuchen die FKIE-Experten bei Schadsoftware. Die prüft üblicherweise vor einer Attacke, ob der ins Visier genommene Rechner bereits infiziert wurde. Falls ja, wird kein Angriff unternommen, um Ressourcen zu sparen. Schadprogramme setzen dazu einen Infektionsmarker, der die Infektion anzeigt. Kennt man solche Marker, kann man diese gezielt einbauen und so das Schadprogramm narren.

Die Arbeiten der Forschungsgruppe Cyber Defense des Fraunhofer FKIE haben vor allem das Ziel, die gesamte Prozess-

kette vom Empfang der Malware über die Analyse bis zu Gegenmaßnahmen drastisch zu beschleunigen. Das ist dringend nötig: Seit 2005 ist die Zahl der neuen Malware-Varianten geradezu explodiert, auf rund 17 Millionen in 2011, sagt das AV-Test-Institut. Bei Stuxnet, mit dem Gerüchten zufolge westliche Geheimdienste eine iranische Atomanlage sabotieren wollten, dauerte die vollständige Analyse des Angriffs etliche Monate. Angesichts der riesigen Zahl von unterschiedlichen Bedrohungen ist dieses Vorgehen viel zu langsam. Eine vollautomatische Erkennung und Beseitigung wird es aber auch in Zukunft nicht geben. Doch die automatisch erhobenen und aufbereiteten Bedrohungsdaten des Cyber Defense Lab machen es Analysten bedeutend leichter.

Die schlechte Nachricht zum Schluss: Hundertprozentige Sicherheit gibt es nicht. Routinierte Angreifer finden immer einen Weg, in ein Rechnersystem einzudringen. Die gute Nachricht: Mit einer ausgefeilten und stets aktuellen Sicherheitsarchitektur kann man es den Angreifern so schwer machen, dass sie die Attacke abbrechen. Denn im Gegensatz zur landläufigen Meinung sind Cyber-Kriminelle meist keine jugendlichen Hacker, die aus Spaß an der Freude handeln, sondern Profis, die für ihre »Arbeit« bezahlt werden und betriebswirtschaftlich denken. Wenn der Aufwand den zu erwartenden Nutzen übersteigt, lohnt sich der Angriff nicht und das ist der beste Schutz.



Sinnbild: Botnet-Operator überwacht und steuert weitere Bots über einen Command-and-Control-Server.

TOR OHNE ZAUN

Elmar Gerhards-Padilla, Leiter der Malware-Analyse am Fraunhofer FKIE, über den Schutz vor Cyber-Attacken.

Wie schützt man seine IT-Infrastruktur am besten?

Indem man das Personal sensibilisiert. Denn in fast der Hälfte der bekannt gewordenen Angriffe sind die eigenen Mitarbeiter das schwächste Glied, das hat eine Untersuchung von Microsoft ergeben. Bekannt sind Fälle, wo Hacker als Putzkolonne getarnt ungehindert in die Firma gelangt sind und vom USB-Stick ein Schadprogramm gestartet haben. Mitunter werden Mitarbeiter zu Mittätern ohne es zu wissen, etwa indem sie einen Dateianhang einer vermeintlich ungefährlichen Mail öffnen. Wissenschaftler bekommen zum Beispiel fast täglich Aufrufe, Vortragsthemen für Konferenzen einzureichen. Sie denken nichts Böses und öffnen solche Dateien, häufig im PDF-Format. Die Täter kennen solche Interessen und nutzen sie gezielt aus. Sie überlegen sich vorher, was den anvisierten Mitarbeiter interessieren könnte und tarnen die Schadsoftware dann in einer entsprechenden Datei.

Betrifft das nicht hauptsächlich große Unternehmen?

Nein. Kleinere Unternehmen glauben, sie hätten keine besonders interessanten Informationen auf ihren Rechnern. Entsprechend lasch gehen sie mit der IT-Sicherheit um. Doch Konstruktionszeichnungen aus der Entwicklung oder Finanzdaten aus dem Controlling können Konkurrenten einen Vorteil verschaffen, der zum Ruin des Opfers führen kann. Hier sehen wir unsere Aufgabe vor allem in der Sensibilisierung der Verantwortlichen.

Häufig wird argumentiert, dass Schutzmaßnahmen den Bedienkomfort von Software minderten.

Sicherheit ist nie der bequemste Weg. Klagen, dass Sicherheitsfunktionen die Bedienung erschweren, sind aus Nutzersicht zwar verständlich, doch die Sicherheitsverantwortlichen sollten den Begehrlichkeiten nicht zu leicht nachgeben. Häufig sind solche Klagen unbegründet, denn auch sichere Systeme können komfortabel zu bedienen sein. Andererseits ist nicht alles, was an Funktionalitäten oder Komfort möglich und wünschenswert wäre, unter Sicherheitsgesichtspunkten auch sinnvoll. So erwarten insbesondere Mitarbeiter aus dem Topmanagement, dass sie jederzeit und von überall Zugriff auf alle Daten haben. Doch das ist gefährlich.

Welche Rolle spielen die Administratoren?

Sie sind nicht immer gute Vorbilder. Administratoren halten sich häufig Türen offen, um für Wartungsarbeiten leichteren Zugriff zu haben. Das kann kurzzeitig sinnvoll sein, wenn diese Ausnahmen dokumentiert und schnell wieder entfernt werden. Doch häufig vergessen die Verantwortlichen dies und lassen so Einfallstore für Angreifer offen. Doch was nützt ein Eisentor, wenn daneben der Zaun fehlt?

Die Devise müsste also lauten: Viel hilft viel?

Man sollte es nicht übertreiben. Uns sind Fälle bekannt, wo sensible Daten aus dem geschlossenen Intranet des Unternehmens schwerer zu erreichen waren als aus dem Internet. Eine gute Sicherheitsarchitektur muss vor externen Angreifern schützen, nicht vor den eigenen Mitarbeitern.

Wie kann die Politik helfen?

Die technischen Mittel zur Abwehr von Malware- und Botnetz-Attacken werden immer besser. Doch damit laufen wir in einen rechtlichen Konflikt. So ist es heute möglich, infizierte Rechner aus der Ferne zu desinfizieren. Doch rechtlich gesehen wäre das ein unerlaubtes Eindringen und damit ebenso strafbar, wie die eigentliche Attacke. Die Politik muss in den nächsten Jahren Rechtssicherheit für die Anbieter von IT-Abwehrdienstleistungen schaffen.

VOM HÖRSAAL ZUM INSTITUT UND ZURÜCK

Am Fraunhofer FKIE wird geforscht – soviel ist klar. Doch wer sind die Mitarbeiter in den Abteilungen und Forschungsgruppen? Und wie sieht eine wissenschaftliche Laufbahn am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE aus?

WEGE IN DIE WISSENSCHAFT

Im Fraunhofer FKIE arbeiten wissenschaftliche Mitarbeiter und Doktoranden, studentische Hilfskräfte und Praktikanten bis hin zu Lehrbeauftragten, Privatdozenten und Professoren. Wir begleiten unsere Mitarbeiter auf ihrem Weg zu Promotion und Habilitation. Die Anstellung im Institut bietet finanzielle Sicherheit, insbesondere aber ein Umfeld, in dem innovative Ideen entstehen und wachsen können. Praxisnahe Projekte für Bund, Länder und die Industrie werfen ständig neue Frage für die Forschung auf, während die tiefe Vernetzung mit der akademischen Welt den intensiven Dialog mit anderen Wissenschaftlern ermöglicht.

VON FRAUNHOFER BIS ÜBERALL HIN

Neben ihrer Anstellung im Institut nehmen zahlreiche Mitarbeiter Lehraufträge unter anderem an den Universitäten Bonn, Aachen und Siegen wahr, haben Lehrstühle inne, betreuen und begutachten Diplom-, Bachelor-, Master- und Doktorarbeiten sowie Habilitationsschriften. Zahlreiche Auszeichnungen für Forschungsarbeiten unserer Mitarbeiter zeigen: Wer eine wissenschaftliche Karriere anstrebt, ist im Fraunhofer FKIE genau richtig. Ob die Tätigkeit im Institut längerfristig ist oder eine Zwischenstation – von hier an stehen alle Wege offen.

Welche Vorteile bringt es mit sich, wenn man abends nach der Arbeit im Hörsaal steht? Eine Antwort von Prof. Dr. Ulrich Schade, Abteilung Informationstechnologie für Führungssysteme (ITF), der neben seiner Tätigkeit im Fraunhofer FKIE seit 2003 außerplanmäßiger Professor an der Universität Bonn ist.

Was machen Sie an der Universität Bonn, Herr Schade?

Ich gebe jedes Semester 2 Semesterwochenstunden im Fach Linguistik. Im letzten Semester war es eine Vorlesung zur Computerlinguistik – zum Beispiel zum Thema maschinelle Sprachverarbeitung. Im Sommersemester 2012 ist es eine Vorlesung zur Klinischen Linguistik – zu Sprachstörungen.

Wie hat die Zusammenarbeit angefangen?

Ich wurde dazu eingeladen, einen Beitrag zur Festschrift zum 60. Geburtstag von Prof. Winfried Lenders vorzutragen. Danach blieb der Kontakt bestehen. Ende 2002 hielt ich einen Vortrag ähnlich einer Antrittsvorlesung und seit 2003 habe ich den Titel »außerplanmäßiger Professor«. Für diesen Titel ist keine Habilitation nötig und man erhält keine Vergütung. Der Titel »Professor« ist – anders als der Doktortitel – abhängig von der Stelle, die besetzt wird.

Was gefällt Ihnen an der Arbeit an der Universität?

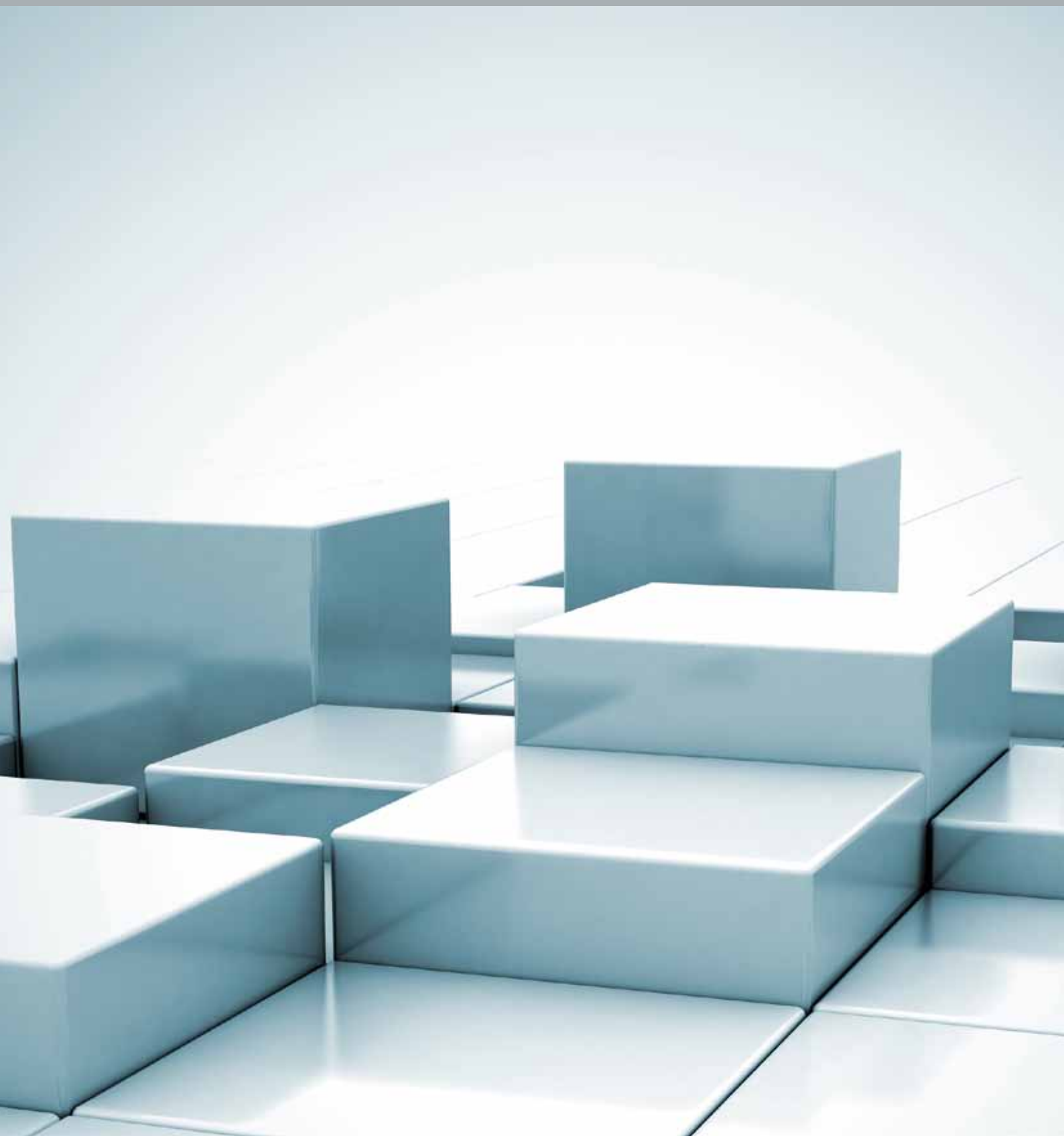
Es macht Spaß. Auch der Titel bringt Vorteile mit sich. Und die Leute, die später für das Institut arbeiten, sind »handpicked«, das heißt sorgfältig von mir ausgewählt. Ich betreue Magisterarbeiten mit Themen, die für das Institut relevant sind. Wichtig sind, speziell für die Abteilung ITF, nicht nur Programmierkenntnisse, sondern auch ein Verständnis für Sprache. Themen sind maschinelle Übersetzung, formale Wissensrepräsentation in Ontologien und semantic roles, für die es viele militärische Anwendungen gibt. Neben Kontakten zur Uni Bonn, deren Studiengänge im ehemaligen Institut für Kommunikationsforschung und Phonetik und im Sprachwissenschaftlichen Institut auslaufen, gibt es nun auch verstärkt Kontakte zum Fach Computerlinguistik an der Uni Bochum. Hier lehrt auch eine meiner ehemaligen Studentinnen.

Wie viele Studenten arbeiten später für das Institut?

Etwa fünfzig Prozent der Mitarbeiter der Abteilung kamen ursprünglich von der Uni Bonn hierher.

WISSENSCHAFTLICHE KARRIERE AM FRAUNHOFER FKIE

DAS KURATORIUM



DAS KURATORIUM

Das Kuratorium begleitet unsere Forschungsarbeit und berät Institutsleiter und den Vorstand der Fraunhofer-Gesellschaft. Die Mitglieder unseres Kuratoriums aus Industrie, Wissenschaft und Ministerien sind:

Vorsitzender
Univ.-Prof. em. Dr.-Ing. Dipl.-Wirt.-Ing. Holger Luczak
RWTH Aachen
Aachen

Prof. Dr.-Ing. Gerd Ascheid
RWTH Aachen
Aachen

Prof. Dr. Armin B. Cremers
Rheinische Friedrich-Wilhelms-Universität
Bonn

Dipl.-Ing. Thomas Dittler, MBA
Dittler & Associates
International Management Consultants GmbH
Schondorf

Prof. Dr. Stefan Fischer
Universität zu Lübeck
Lübeck

Prof. Dr.-Ing. Uwe Hanebeck
Karlsruher Institut für Technologie KIT
Karlsruhe

Dr.-Ing. Hans-Joachim Kolb
MEDAV GmbH
Uttenreuth

Dipl.-Ing. Herbert Rewitzer
ROHDE & SCHWARZ GmbH & Co. KG
München

Prof. Dr.-Ing. Axel Schulte
Universität der Bundeswehr München
Neubiberg

MinDirig Dr. Dietmar Theis
BMVg - Bundesministerium der Verteidigung
Bonn

Thomas Tschersich
IT-Security Deutsche Telekom AG
Bonn

Dr. Uwe Wacker
EADS – Deutschland GmbH
Ulm

MinR Dipl.-Ing. Norbert Michael Weber
BMVg – Bundesministerium der Verteidigung
Bonn

Prof. Dr.-Ing. Klaus Wehrle
RWTH Aachen
Aachen

Dr. Thomas H. G. G. Weise
Rheinmetall AG
Düsseldorf

FRAUNHOFER-GESELLSCHAFT

Forschen für die Praxis ist die zentrale Aufgabe der Fraunhofer-Gesellschaft. Die 1949 gegründete Forschungsorganisation betreibt anwendungsorientierte Forschung zum Nutzen der Wirtschaft und zum Vorteil der Gesellschaft. Vertragspartner und Auftraggeber sind Industrie- und Dienstleistungsunternehmen sowie die öffentliche Hand.

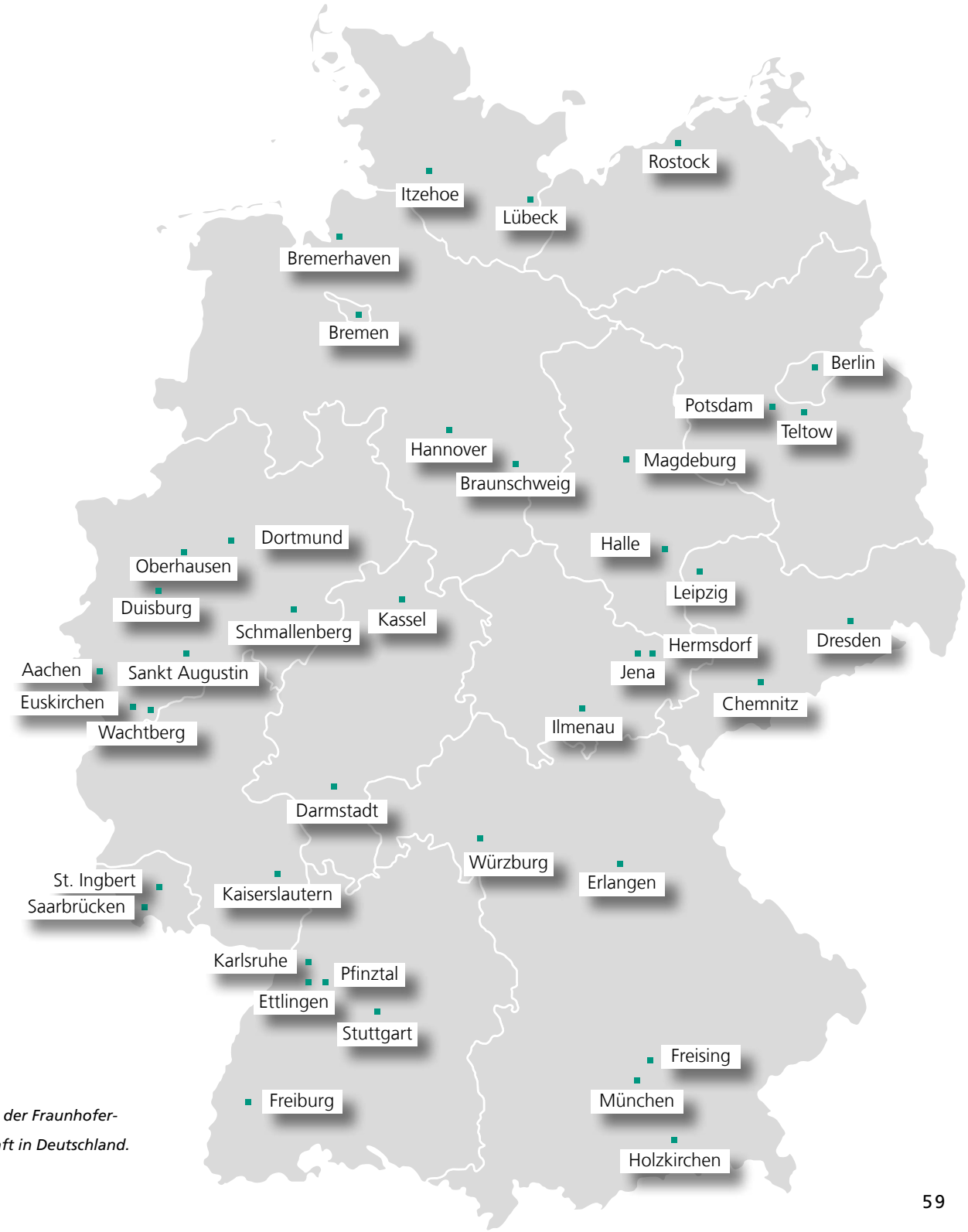
Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit mehr als 80 Forschungseinrichtungen, davon 60 Institute. Mehr als 18 000 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, bearbeiten das jährliche Forschungsvolumen von 1,65 Milliarden Euro. Davon fallen 1,40 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Zwei Drittel dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Nur ein Drittel wird von Bund und Ländern als Grundfinanzierung beigesteuert, damit die Institute Problemlösungen erarbeiten können, die erst in fünf oder zehn Jahren für Wirtschaft und Gesellschaft aktuell werden.

Internationale Niederlassungen sorgen für Kontakt zu den wichtigsten gegenwärtigen und zukünftigen Wissenschafts- und Wirtschaftsräumen.

Mit ihrer klaren Ausrichtung auf die angewandte Forschung und ihrer Fokussierung auf zukunftsrelevante Schlüsseltechnologien spielt die Fraunhofer-Gesellschaft eine zentrale Rolle im Innovationsprozess Deutschlands und Europas. Die Wirkung der angewandten Forschung geht über den direkten Nutzen für die Kunden hinaus: Mit ihrer Forschungs- und Entwicklungsarbeit tragen die Fraunhofer-Institute zur Wettbewerbsfähigkeit der Region, Deutschlands und Europas bei. Sie fördern Innovationen, stärken die technologische Leistungsfähigkeit, verbessern die Akzeptanz moderner Technik und sorgen für Aus- und Weiterbildung des dringend benötigten wissenschaftlich-technischen Nachwuchses.

Ihren Mitarbeiterinnen und Mitarbeitern bietet die Fraunhofer-Gesellschaft die Möglichkeit zur fachlichen und persönlichen Entwicklung für anspruchsvolle Positionen in ihren Instituten, an Hochschulen, in Wirtschaft und Gesellschaft. Studierenden eröffnen sich an Fraunhofer-Instituten wegen der praxisnahen Ausbildung und Erfahrung hervorragende Einstiegs- und Entwicklungschancen in Unternehmen.

Namensgeber der als gemeinnützig anerkannten Fraunhofer-Gesellschaft ist der Münchner Gelehrte Joseph von Fraunhofer (1787 – 1826). Er war als Forscher, Erfinder und Unternehmer gleichermaßen erfolgreich.



Standorte der Fraunhofer-Gesellschaft in Deutschland.

WISSENSCHAFTLICHE BERICHTE

FKIE-Bericht-Nr.	Titel	Verfassung	Monat
207	Multilinguale Inhaltserschließung mit semantischem Schlussfolgern auf militärisch relevanten Texten (mIE-Projekt)	Hecking, M. ; Wotzlaw, A. ; Coote, R.	Jan.
208	System description and first experimental results of the Gamma GSM passive radar	Zemmari, R.	Jan.
209	Integrated GMTI Radar and Report Tracking for Ground Surveillance	Keong, Chan Ho ; Ulmke, M. ; Koller, J.	Jan.
210	Adaptive Tracking with a Multifunction Radar: Theoretical Framework and Implementation Issues	Hügel, M. ; Koch, W.	März
211	Annotation semantischer Ambiguitäten in militärisch relevanten Texten des Englischen	Hegele, S.	März
212	Efficient and Portable Waveform Development for Software Defined Radios	Ramakrishnan, V. Adrat, M. ; Deidersen, U.	April
213	Beiträge zur passiven Zielentdeckung und Clutterunterdrückung mit Mobilfunk-Signalen	Wirth, W.-D.	Juli
214	Accuracy Study and State Estimation for Piecewise Maneuvering Targets with Unknown Maneuver Change Times	Hörst, J. ; Oispuu, M.	Juli.
215	KOM – Eingeschränkter Benutzerkreis.	–	
216	Methodische Vorgehensweise bei der ergonomischen Gestaltung von Benutzungsschnittstellen zur Nutzung der STANAG 2019 NATO JOINT MILITARY SYMBOLS	Kaster, A. ; Ruckert, C. ; Träber, S. ; Becker, R.	Dez..

			Monat
217	Untersuchung zum Einfluss der Interaktionsmodalität auf die Telekooperation bei der Instandsetzung	Pfendler, C. ; Thun, J. ; Alexander, T.	Nov.
218	Advanced Tracking and Fusion Methods for Ground Surveillance	Mertens, M. ; Ulmke, M. ; Feldmann, M. ;	Nov.
219	A Sequential Monte Carlo Method for Multi-Target Tracking with the Intensity Filter	Schikora, M. ; Koch, W. ; Streit, R. ; Cremers, D.	Nov.
220	Detecting Anomalies in Sensor Signals Using Database Technology	Schüller, G. ; Behrend, A. ; Koch, W.	Dez.
221	Two spezial cases of classification in images: Pixel-based and Region-based	Madhogaria, S. ; Schikora, M.	Dez.
222	Modellierung und Simulation zur Erfassung und Analyse von urbanen Operationen	Alexander, T. ; Renkewitz, H. ; Schimanski, S. ; Zamborlini, B.	Dez.
223	Ergonomie der Informationsdarstellung für mobile Einsatzkräfte	Pfendler, C. ; Brandt, M. ; Kinder, V. ; Renkewitz, H. ; Alexander, T.	Nov.

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

SDF

Verfasser	Titel
Daun, D.; Nickel, U.; Koch, W.	Tracking in Multistatic Passive Radar Systems Using DAB/ DVB-T Illumination. Signal Processing, 92(2012)pp. 1365–1386
Daun, M.; Brötje, L.; Ehlers, F.	Simultaneous Localisation and Tracking' onboard AUVs with Multistatic Sonar Data. In: UAM 2011. 4th International Conference and Exhibition on Underwater Acoustic Measurements. Technologies and Results. Kos: 20.–24. June 2011
Demissie, B.	Direct Localization and Detection of Multiple Sources in Multi-Path Environments. In: Fusion 2011. 14th International Conference on Information Fusion. Chicago: 5.– 8. July 2011. IEEE Press, 2011, 8 pp. (ISBN 978-0-9824438-2-8)
Engel, U.; Okum, M.	On The Application of the Higher Order Virtual Array Concept for Small Antenna Arrays. In: EUSIPCO-2011. Proceedings of 19th ... . European Signal Processing Conference. Barcelona: 29. August – 2. September 2011. EURASID, 2011, pp. 609 – 613 (ISSN 2076-1465)
Feldmann, M.; Fränken, D.; Koch, W.	Tracking of Extended Objects and Group Targets Using Random Matrices. IEEE Transactions on Signal Processing, 59 (2011) pp. 1409–1420
Govaers, F.; Koch, W.	Exact Out-of-Sequence Processing Using the Information Filter. In: Fusion 2011. 14th International Conference on Information Fusion. Chicago: 5.–8. July 2011. IEEE Press, 2011, 7 pp. (ISBN 978-0-9824438-2-8)
Häge, M.; Oispuu, M.	DOA and Polarization Accuracy Study for an Imperfect Dual-Polarized Antenna Array. In: EUSIPCO-2011. Proceedings of 19th ... . European Signal Processing Conference. Barcelona: 29. August – 2. September 2011. EURASID, 2011, pp. 599– 603 (ISSN 2076-1465)
Koch, W.; Govaers, F.	On Accumulated State Densities with Applications to Out-of-Sequence Measurement Processing. IEEE Transactions on Aerospace and Electronic Systems, 47(2011)pp. 2766–2778
Nickel, U.; Chaumette, E.; Larzabal, P.	Statistical Performance Prediction of Generalized Monopulse Estimation. IEEE Transactions on Aerospace and Electronics Systems, 47(2011)pp. 381–404
Schikora, M.; Oispuu, M.; Koch, W.; Cremers, D.	Multiple Source Localization Based on Biased Bearings Using the Intensity Filter – Approach and Experimental Results. In: CAMSAP'2011. 4th IEEE Intl. Workshop on Computational Advances in Multi-Sensor Adaptive Processing. San Juan: 13. – 16. December 2011. pp. 61 – 64 (ISBN 978-1-4577-2104-5)
Schüller, G.; Saul, R.; Behrend, A.	In-Memory Caching for Fast Stream History Access. In: IWGS ,11 Proceedings of the 2nd ACM SIGSPAT IAL International Workshop on GeoStreaming. Chicago: 1.–4. November 2011. ACM Press, 2011, pp. 37 – 40 (ISBN 978-1-4503-1036-9)

Verfasser	Titel
Wirth, W.-D.	Joint Application of Autocalibration, Superresolution and Blind Multipath Estimation with an Experimental Array. IET Signal Processing, 5 (2011) pp. 426– 432
Zemmari, R.	Time Jitter Influence on GSM Passive Radar. In: IRS 2011. 12th International Radar Symposium. Dresden: 7.– 9. September 2011. DGON German Institute of Navigation, 2011, pp. 292–300. (ISBN: 978-3-927535-28-2)
Aschenbruck, N.; Fuchs, C.	STMP – Sensor Data Transmission and Management Protocol. In: LCN 2011. Proc. of the 36th IEEE Conference on Local Computer Networks. Bonn: 4.–7. October 2011. IEEE Press, 2011, S. 475–483 (ISBN 978-1-61284-928-7)
	An Integrated Simulation Environment for Sensor Data Fusion Applications in Wireless Mesh Networks. In: IEEE MILCOM 2011. Proc. of the Military Communications Conference. Baltimore: 7.–10. November 2011. IEEE Press, S. 1778–1783 (ISBN 978-1-4673-0081-0)
Barz, C.; Jansen, N.	Towards a Middleware for Tactical Military Networks – Interim Solutions for Improving Communication for Legacy Systems. In: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 289–297 (ISBN 978-83-62954-20-9)
Couturier, S.	Cognitive Radio as Enabling Technology for Dynamic Spectrum Access. In: Emerged/Emerging »Disruptive« Technologies (E2DT). Paper presented at the RTO Information Systems Technology Panel (IST) Symposium. Madrid: 9.–10. May 2011. NATO, RTO, 2011, RTO-MP-IST-99 (ISBN 978-92-837-0147-7)
Couturier, S.; Adrat, M.; Bosch, T.; Leduc, J.; Singh, S.; Antweiler, M.	Evaluation of Wireless Civilian Communication Systems for Military Applications. In: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 81–91 (ISBN 978-83-62954-20-9)
Damm, D.; Grohganz, H.; Kurth, F., Ewert, S.; Clausen, M.	SyncTS: Automatic synchronization of speech and text documents. In: AES 42nd International Conference Semantic Audio. Ilmenau: 22.–24. July 2011. AES Press, 2011, S. 98–107 (ISBN 978-0-937803-81-3)
Demissie, B.; Kreuzer, S.	Uniform Blind Equalization of Two-Path Channels with Zeros on the Unit Circle. In: 19th European Signal Processing Conference (EUSIPCO). Barcelona: 29. August– 2. September 2011. EURASIP, 2011, S . 2200–2204 (ISSN 2076-1465)
Demissie, B.; Kreuzer, S.	Performance Predictions for Parameter Estimators that Minimize Cost-Functions using Wirtinger Calculus with Application to CM Blind Equalization. IEEE Transactions on Signal Processing, 59 (2011) pp. 3685–3698

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

Verfasser	Titel
Ginzler, T.	A robust and scalable publish/subscribe mechanism for peer-to-peer networks. Warschau: Military University of Technology, Ph.D.-Diss., 2011
Goetz, M.; et al.	Jamming-Resistant Multi-path Routing for Reliable Intruder Detection in Underwater Networks. In: WUWNet 2011. The 6th ACM International Workshop on UnderWater Networks. Seattle: 1.–2. December 2011. ACM Press, 2011, 5 pp. (ISBN 978-1-4503-1151-9)
Ramakrishnan, V.; Veerkamp, T.; Adrat, M.; Ascheid, G.; Antweiler, M.	Implementations of Sorted-QR Decomposition for MIMO Receivers: Complexity, Reusability and Efficiency Analysis. Journal of Signal Processing Systems, (2012)
Schmalen, L.; Adrat, M.; Clevorn, T.; Vary, P.	EXIT Chart Based System Design for Iterative Source-Channel Decoding with Fixed-Length Codes. IEEE Transactions on Communications, 59(2011) pp. 2406–2413
ITF	
Barz, C.; Jansen, N.	Towards a Middleware for Tactical Military Networks – Interim Solutions for Improving Communication for Legacy Systems. in: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 289–297 (ISBN 978-83-62954-20-9)
Gerz, M.; Meyer, O.	Defining C2 semantics by a platform-independent JC3IEDM. International Journal of Intelligent Defence Support Systems, 4(2011)3, S. 263–285
Haarmann, B.; Schade, U.	Grammar Research that supports SISO C-BML Phase 2. In: BML (Battle Management Language) Research Symposium. Boston: 8. April 2011. Proceedings, 23 pp. http://c4i.gmu.edu/events/conferences/2011/BMLsymposium2011/
Haarmann, B.; Sikorski, L.; Schade, U.	Text Analysis beyond Keyword Spotting. In: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 355 – 365 (ISBN 978-83-62954-20-9)
Lang, B.; Gerz, M; Meyer, O.; Sim, D.	An Enterprise Architecture for the Delivery of a Modular Interoperability Solution. In: Semantic and Domain-based Interoperability. Paper presented at the RTO Information Systems Technology Panel (IST) Symposium. Oslo: 7.– 8. November 2011. NATO – RTO, 2011, RTO-MP-IST-101 (ISBN 978-92-837-0160-6)
Noubours, S.; Hecking, M.	Semantic Analysis of Military Relevant Texts for Intelligence Purposes. in: 16th ICCRTS. International Command and Control Research and Technology Symposium. Quebec: 21.– 23. June 2011. CCRP Press, 2011, Paper 19
Rein, K.	A Simple Heuristics-Based Model for Threat Prediction to Support Decision-Making. The International C2 Journal, 5(2011)1, S.1–26

Rein, K.; Schade, U.	Making Molehills out of Mountains: A Methodology for Shallow Processing for Text-Based Information Fusion. In: International Conference on Soft Computing and Applications (ICSCA'11). San Francisco: 19.– 21. October 2011
Remmersmann, T.;	Coordinating Ambulance Operations. In: Future Security: 6th Security Research Conference.
Rein, K.; Schade, U.	Berlin: 5.–7. September 2011. Ender, J.; u.a. (Eds.), Fraunhofer Verl., 2011, S. 47–50 (ISBN 978-3-8396-0295-9)
Schade, U.; Haarmann, B.; Hieb, M.R.	A Grammar for Battle Management Language. In: DS-RT '11. Proceedings of the 2011 IEEE/ACM 15th International Symposium on Distributed Simulation and Real Time Applications. IEEE/ACM Press, 2011, S. 155 – 159 (ISBN: 978-1-4577-1643-0)
Wunder, M. et al.	Semantic Interoperability. In: Semantic and Domain-based Interoperability. Paper presented at the RTO Information Systems Technology Panel (IST) Symposium. Oslo: 7.– 8. November 2011. NATO – RTO, 2011, Paper 15, RT O-MP-IST-101 (ISBN 978-92-837-0160-6)
Alexander, T.; Conradi, J.	On the Applicability of Digital Human Models for Personal Equipment Design. In: HCI International 2011. Part II. Orlando: 9.–14. July 2011. Springer, 2011, pp. 315–319 (Communications in Computer and Information Science; 174), (ISBN 978-3-642-22094-4)
Becker, R.; Ruckert, C.	Methodisches Design von Mensch-Maschine-Schnittstellen unter Berücksichtigung nutzerzentrierter und modellbasierter Ansätze. In: Reflexionen und Visionen der Mensch-Maschine-Interaktion. 9. Berliner Werkstatt. Mensch-Maschine-Systeme. Berlin: 5.–7. Oktober 2011. VDI Verlag, 2011, S. 42–43 (VDI Fortschritt-Berichte: Mensch-Maschine-Systeme; 33) (ISBN 978-3-18-303322-5)
Dalinger, E.; Ley, D.	A Reference Model for Designing Decision Support Systems in Novel Work Domains, In: IEEE SMC 2011. Proceedings of the IEEE Int. Conf. on Systems, Man and Cybernetics. Anchorage: 9.–12. October 2011. IEEE Press, 2011, pp. 1615–1620 (ISBN 978-1-4577-0652-3)
Kleiber, M.; Alexander, T.	Evaluation of a Mobile AR Tele-Maintenance System. In: Universal Access in Human-Computer Interaction. Applications and Services. 6th International Conference. UAHCI 2011. Held as Part IV of HCI International 2011. Orlando: 9.–14. July 2011. Springer, 2011,pp. 253–262 (Lecture Notes in Computer Science; 6768) (ISBN 978-3-642-21656-5)
Kruger, F.; Kleiber, M.; Schlick, C.M.	System for a model based analysis of user interaction patterns within web-applications. In: IEEE SMC 2011. Proceedings of the IEEE Int. Conf. on Systems, Man and Cybernetics. Anchorage: 9.–12. October 2011. IEEE Press, 2011, pp. 1274–1279 (ISBN 978-1-4577-0652-3)

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

Verfasser	Titel
Ley, D.	Expert-Sided Workflow Data Acquisition by Means of an Interactive Interview System. In: Human Centered Design. 2nd Intl. Conference. HCD 2011. Held as Part of HC I International 2011. Orlando: 9.–14. July 2011. Springer, 2011, pp. 91–100 (LNCS 6776) (ISBN 978-3-642-21752-4)
Ley, D.; Dalinger E.	Security Modeling Technique: Visualizing Information of Security Plans. TransNav – International Journal on Marine Navigation and Safety of Sea Transportation, 5 (2011) pp. 417–422
Ruckert, C.; Becker, R.; Kaster, A.	Modellbasierte und nutzerzentrierte Methodik zur systematischen Erhebung natürlich-sprachlicher Anforderungen für Mensch-Maschine-Schnittstellen. In: Ergonomie im interdisziplinären Gestaltungsprozess. 53. Fachausschusssitzung Anthropotechnik. Neu-Isenburg: 27.– 28. Oktober 2011. DGLR, 2011. (DGLR-Bericht ; 2011-01) (ISBN 978-3-932182-75-8)
Winkelholz, C.; Kleiber, M.	Age Dependent Differences in the Usage of a Desktop VR System for Air Force Mission Planning and Preparation. In: Universal Access in Human-Computer Interaction. Applications and Services. 6th Intl. Conference. UAHCI 2011. Held as Part of HCI International 2011. Orlando: 9.–14. July 2011. Springer, 2011, pp. 292–300. (LNCS 6768) (ISBN 978-3-642-21656-5)
US	
Brunner, M.; Schulz, D.; Cremers, A.B.	Adhering to terrain characteristics for position estimation of mobile robots In: Informatics in Control, Automation and Robotics 2010. Revised and selected papers. Funchal: 15.–18. June 2010. Berlin: Springer, 2011, pp. 153–169 (Lecture Notes in Electrical Engineering; 89) (ISBN: 978-3-642-19538-9)
Brunner, M.; Höller, F.; Königs, A.; Röhling, T.; Schneider, F.E.; Tiderko, A.; Schulz, D.; Wildermuth, D.	The FKIE Robot System for the European Land Robot Trial 2011. In: RISE'2011. Robotics for Risky Interventions and Environmental Surveillance-Maintenance. Fifth International Workshop on … . Brüssel: 17.–18. June 2011.
Königs, A.; Schulz, D.	Fast Visual People Tracking using a Feature-Based People Detector. In: Intelligent Robots and Systems. IROS 2011. IEEE/RSJ International Conference on … . : San Francisco: 25.–30. September 2011. IEEE Press, 2011, pp. 3614–3619 (ISBN 978-1-61284-454-1)
Oehler, B.; Stückler, J.; Welle, J.; Schulz, D.; Behnke, S.	Efficient Multi-Resolution Plane Segmentation of 3D-Point Clouds, In: ICIRA 2011. Intelligent Robotics and Applications. 4th International Conference. Aachen: 6.–8. December 2011. Springer, 2011, pp. 145–156 (Lecture Notes in Computer Science; 7102) (ISBN 978-3-642-25489-5)
Schneider, F.E.; Wildermuth, D.	Evaluating the Effect of Robot Group Size on Relative Localisation Precision. In: TAR OS 2011. Towards Autonomous Robotic Systems 2011. 12th Annual Conference. Sheffield: 31. August – 2. September 2011. Springer, 2011, pp. 149 –160 (ISBN 978-3-642-23231-2)

Schöler, F.; Behley J.; Steinhage, V.; Schulz, D.; Cremers, A.B.	Person tracking in three-dimensional laser range data with explicit occlusion adaption; In: Robotics and Automation (ICRA) 2011. IEEE International Conference on … . Shanghai: 9. – 13. May 2011. IEEE Press, 2011, pp. 1297–1303 (ISBN: 978-1-61284-386-5)

CD

Aurisch, T.; Ginzler, T.; Steinmetz, P.	Handling Merge and Disruption of Mobile Ad Hoc Networks in a Secure Tactical Instant Messaging System. In: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 471– 481 (ISBN 978-83-62954-20-9)
Aurisch, T.; Steinmetz, P.	Securely connecting instant messaging systems for ad hoc networks to server based systems. In: 16th ICCRTS . International Command and Control Research and Technology Symposium. Quebec: 21.– 23. June 2011. CCRP Press, 2011, Paper 36
Czosseck, C.; Klein, G.; Leder, F.	On the arms race around botnets – setting up and taking down botnets. In: ICCC 2011. 3rd International Conference on Cyber Conflict. Tallinn: 7. – 10. June 2011. IEEE Press, 2011, 14 pp. (ISBN 978-9949-9040-2-0)
Gerhards-Padilla, E.; Aschenbruck, N.; Martini, P.	TOGBAD – An Approach to Detect Routing Attacks in Tactical Environments. Security and Communication Networks, 4 (2011) pp. 793–806
	Wormhole Detection using Topology Graph based Anomaly Detection (TOGBAD). In: WMAN 2011. Proc. of the 6th Workshop on Wireless and Mobile Ad-Hoc Networks. Kiel: 10.–11. March 2011. Electronic Communications of the EASST – a peer-reviewed, scientific and open access journal (2011) Vol. 37: Kommunikation in Verteilten Systemen – 2011, 12 pp. (ISSN 1863-2122)
Hommen, J.; Klein, G.; Rogge, H.; Jahnke, M.; Grebe, A.	Detection of IEEE 802.11 MAC-layer Frame Collisions in a MANET Emulation Environment. In: MCC 2011. Military Communication and Information Technology. Amsterdam: 17.–18. October 2011. Military Univ. of Technology, 2011, S. 483–494 (ISBN 978-83-62954-20-9)
Klein, G.; Tölle, J.; Martini, P.	From detection to reaction – A holistic approach to cyber defense In: DRS 2011. Defense Science Research Conference and EXPO. Singapore: 3.– 5. August 2011. IEEE Press, 2011, 4 pp. (ISBN 978-1-4244-9276-3)
Plohmann, D.; Leder, F.; Gerhards-Padilla, E.; Gassen, J.; Wichmann, A.; Eschweiler, S.	Botnets: Detection, Measurement and Defense. In: Future Security: 6th Security Research Conference. Berlin: 5.–7. September 2011. Ender, J. ; u.a. (Eds.) Fraunhofer Verl., 2011, S. 562–567 (ISBN 978-3-8396-0295-9)
Tölle, J.; Jahnke, M.; Klein, G.	Lagedarstellung für Cyber Defense: Was ist los im Netz In: AFCEA 2011 – Fraunhofer-Institute. Behörden Spiegel, Mai 2011, S. 54 – 55, Sonderheft (ISBN 978-3-934401-15-0)

TÄTIGKEIT IN GREMIEN DER NATO

Beitragende	Tätigkeit
Abut, F.; Aurisch, T.; Barz, C.; Bongartz, H.; Diefenbach, A.; Ginzler,T.; Schmidt, H.; Sevenich, P.; Steinmetz, P.; Tölle, J.; Wilmes, M.	Multinationales FuT Projekt CoNSIS »Coalition Network for Secure Information Sharing«
Adrat, M.	NATO C3SNR Coalition Wideband Networking Waveform (COALWNW)
Alexander, T.; Kaster, A.	EDA: CAPTECH ESM 04 (Human Factors & CBR Protection), Government Experts
Alexander, T.	EDA: CAPTECH ESM 04 Strategic Research Agenda, Government Expert NATO RTO HFM-165/RTG on Improving Human Effectiveness through Embedded Virtual Simulation, Chairman NATO RTO HFM-216/RTG on Synthetic Environments for HSI Application, Assessment and Improvement, German Member NATO RTO NMSG-107 RWS on Human Behavior Modeling for Military Training Applications, German Member
Barz, C.	NATO RTO IST-909 on «SOA-Challenges for Real-Time and Disadvantaged Grids«
Barz, C.; Rogge, H.	EU FP7 ICT Large-Scale Integrated Projekt CONFINE »Community Networks Testbed fort he Future Internet«
Bau, N.; Schüller, H.	Teilnahme am 5 Power Net-Centric Project Arrangement (5P NC PA)
Bosch, T.	NATO IST-ET-065 Dynamic Wireless Network Cross-layer Security and Security Awareness in Coalition Environments
Brüggemann B.; Königs, A.	Teilnahme an der NAT O NIAG Studie SG-157
Brüggemann, B.	Besuch ET SCI 251
Couturier, S.	NATO RTO/IST-077 RT G-035 Cognitive Radio in NATO
Couturier, S.; Adrat, M.; Liedtke, F.	NATO RTO/SCI-222 Electronic Warfare Issues of Software Defined Radio
Gerz, M.; Kaster, J.; Schüller, H.; Huy, S.	Teilnahme an und Auswertung der Coalition Warrior Interoperability Exercise (CWIX 2011)
Gerz, M.; Bau, N.; Busch, C.; Schüller, H.	Teilnahme und Leitung von Arbeitsgruppen des Multilateral Interoperability Programme (MIP)

Gerz, M.	Mitglied des Technical Program Committee für das IST-101 / RSY-024 Symposium »Semantic & Domain based Interoperability«, Oslo, November-2011.
Goetz, M.; Gerharz, M.	Projekt Robust Acoustic Communication in Underwater Networks (RACUN)
Grosche, J.	NATO RTO IST Panel-Member
Hecking, M.	NATO IST-078/RT G-036 Machine Translation for Coalition Operations
Hunke, S.; Bosch, T.	NATO/RTO Exploratory Team on Security in Mobile Ad-hoc Networks, IST-081/ET-065.
Jansen, N.	NATO IST-090/RT G-043 Service Oriented Architecture (SOA) Challenges for Real Time and Disadvantaged Grids
Kleiber, M.	NATO IST-085, RT G-041: Interactive Visualisation of Network Dynamics, NAT O-Arbeitsgruppe
Leduc, J.	NATO C3B SC/6 Ad-Hoc Working Group/2 on V/UHF Communications NATO-AHWG/2-Expertenteam zur Entwicklung von Schmalbandwellenformen
Leduc, J.; Adrat, M.	JCGUAV Support Team »Interoperable Command & Control Data Link for UAV « (IC2DL), STANAG 4660
Leduc, J.; Couturier, S.; Bosch, T.	EDA PT Software Defined Radio
Rogge, H.	IETF WG Wireless Mesh Networks
Schade, U.; Rein, K.; Remmersmann, T.	NATO RTO MSG-085 Standardization of C2-Simulation Interoperability
Wunder, M.	NATO Research & Technology Organisation, Deutscher Vertreter im IST-Panel Symposium Chairman, Moderator und Organisator des NAT O-Symposiums IST-101/RSY-024 Domain based and Semantic Interoperability, Oslo 7/9-Nov-2011 Chairman der NAT O-Arbeitsgruppe IST-094/RT G-044 Framework for Semantic Interoperability Technical Program Committee Member und Session Chairman, Military Communications and Information Systems Conference, Amsterdam 17/18-Okt-2011
Ulmke, M.	Technical Team Member, NAT O RT O SET-142 »Acoustics and Autonomous Sensing for ISP Applications«

IMPRESSUM

HERAUSGEBER
Fraunhofer-Institut für Kommunikation,
Informationsverarbeitung und Ergonomie FKIE

Neuenahrer Str. 20
53343 Wachtberg

Tel.: +49 (0)228 9435-287
Fax: +49 (0)228 9435-685

fkie@fkie.fraunhofer.de
www.fkie.fraunhofer.de

REDAKTION
Bernd Müller, Dr. Michael Gerharz, Bernhard Kleß

LAYOUT, SATZ, LEKTORAT
Volker Kurzidim, FKIE-Stabstelle

FOTOGRAFIE
Uwe Bellhäuser / das bilderwerk

BILDQUELLEN
Bilder © Fraunhofer FKIE.

Ausnahmen:
S.13/14: Piktogramme: Generiert mit der Visualisierungssoftware Geo4T der Firma *Schönhofer Sales & Engineering*
S.18, S.22 - S.25/31: Informations- und Medienzentrale der Bundeswehr: Combined Endeavour 2005
S.30: Press and Information Department Ministry of National Defence Republic of Poland / Foto: *NATO Coalition Warrior Interoperability Exercise (CWIX), June 2011, Bydgoszcz, Poland*

Lizenzen:
S.27: Understanding highligted in dictionary, istockphoto
S.51: Source Code, Fotolia
S.52: botnet mit bot herder 3D © Gunnar Assmy, Fotolia
S.56: Abstract box background, Fotolia

Future Security
Security Research Conference

FRAUNHOFER GROUP FOR DEFENSE AND SECURITY

Fraunhofer VVS

7TH FUTURE SECURITY, BONN, 4TH – 6TH SEPTEMBER, 2012

CONFERENCE CHAIR
Prof. Dr. Peter Martini, Fraunhofer FKIE

PROGRAM CO-CHAIRS
Prof. Dr. Michael Meier, University of Bonn
Prof. Dr. Nils Aschenbruck, University of Osnabrück

LOCAL ARRANGEMENTS CHAIR
Hans-Peter Stuch, Fraunhofer FKIE

WWW.FUTURE-SECURITY.EU